Advanced Technical Reference Guide
VPN-1/FireWall-1®

Check Point 2000

If you are reading this in a PDF file
Note that the entries in this *Table of Contents* are not links. To jump to a section use the bookmarks in the left pane

Contents

Preface
Scope…1
Links to SecureKnowledge and Other Places…1
Who should use this Guide…1
How to obtain the latest version of this Guide…2
Feedback Please!…2
Summary of Contents…2

Chapter 1: Troubleshooting Overview
Troubleshooting Guidelines…3
Information to Gather…3

Chapter 2: Troubleshooting Tools
fwinfo…6
VPN-1/FireWall-1 Control Commands…8
FireWall-1 Monitor Command…16
Debugging with INSPECT…19
More Information…20

Chapter 3: Troubleshooting Network Address Translation
Introduction…22
Resolving Common NAT Problems…22
Debugging NAT…28
More Information…28

Chapter 4: Troubleshooting Routers and Embedded Systems
Introduction…30
Management Server Architecture…30
VPN-1/FireWall-1 configuration for a Nortel (Bay Networks) BayRS router…31
VPN-1/FireWall-1 configuration for a Xylan switch…38
Debugging Routers and Embedded…39
More Information…40

Chapter 5: Troubleshooting Open Security Extension
Introduction…42
Nortel (Bay) Routers: Configuration and Problem Resolution…42
Cisco Routers: Problem Resolution and Debugging…44
Cisco Pix Firewall: Problem Resolution…45
3COM routers: Problem Resolution and Debugging…46
Microsoft RRAS (SteelHead) Routers: Problem Resolution and Debugging…47
More Information…47

If you are reading this in a PDF file
Note that the entries in this *Table of Contents* are not links. To jump to a section use the bookmarks in the left pane

Chapter 6: Troubleshooting Anti-Spoofing

Introduction…49
Common Problems Resolution…49
Debugging Anti-Spoofing…51

Chapter 7: Troubleshooting Security Servers and Content Security

HTTP Security server…54

How to Improve HTTP Security Server performance in a High Performance Environment…54
Resolving Common HTTP Security Server Problems…59
Troubleshooting Security Server Performance problems…63

FTP Security Server…66

The FTP security server…66
Resolving Common FTP security server problems…66

SMTP Security Server…71

SMTP Email Process…71
The SMTP Security Server Process…72
Troubleshooting Common SMTP Security Server problems…73
Understanding the error handling mechanism of the SMTP daemon…74
How SMTP Security Server deals with envelope format…75
Log Viewer Error Messages…75
What commands are supported by the VPN-1/FireWall-1 SMTP Security Server?…77

Debugging Security servers…78

More Information: Security servers and content Security…79

Chapter 8: Troubleshooting LDAP Servers and the AMC

Introduction…81
Troubleshooting LDAP Issues…82
Installation Issues…83
Configuration Issues…83
Known configuration problems…85
Working with the AMC…87
Working with LDAP…89
Known LDAP and AMC problems…89
Special Configurations…91
PKI Issues related to LDAP…91
Known Limitations…92
Debugging LDAP…93
More Information…95

Chapter 9: Troubleshooting Active Network Management

Troubleshooting Synchronization…98

Synchronization and High Availability…98
Resolving Common Synchronization Problems…100

Troubleshooting Fail-over…101

Fail-over in High Availability Applications…101
Debugging High-Availability…106

Troubleshooting Load Balancing…107

How Server Load Balancing Works…107
Load Balancing Components…107
License requirement for Load Balancing…107
Load Balancing Configuration Guides…108
Resolving Common Load Balancing problems…108
Debugging the Connect Control Module…109
Debugging the Load Balancing daemon lhttpd…112
Debugging the Server-Load Load balancing algorithm…112

Chapter 10: Troubleshooting SNMP

Introduction…115
How to configure HP Open View to work with FireWall-1 4.0…115
Resolving Common SNMP Problems…115
More Information…116

Chapter 11: Troubleshooting Licensing

Check Point Licensing Policy…118
Product Features Lists…121
Resolving Common Licensing Problems…122

Chapter 12: What To Send Technical Support

Introduction…128
Rule Base…128
Network Address translation…128
Anti Spoofing…128
INSPECT…129
GUI…129
LOG…129
High Availability…130
Security Servers…130
LDAP…131
Routers and Embedded Systems (OEM)…131
Open Security Extension (OSE)…132
Crashes…132

Chapter 13: Check Point Support Information

Mission Statement…134
Check Point Worldwide Technical Services General Process…134
Availability of Check Point Worldwide Technical Services…134
Contacting Check Point Worldwide Technical Services by Telephone…134
Contacting Check Point Worldwide Technical Services by E-mail…136
Problem Severity Definitions…137
Software Versions Supported…137
Escalation Procedure…137

Appendix A: State Tables for VPN-1/FireWall-1 4.0

What are State Tables?…141

The basic structure of a connection in a table entry…142
General tables…143
SAMP tables…147
License enforcement tables…148
Logging tables…149
NAT tables…151
VPN tables…153
SecuRemote — client side tables…157
SecuRemote — server side tables…159
Security Server and Authentication tables…162
Load balancing tables…165
Specific services tables…167
RPC tables…169
DCE/RPC tables…171
IIOP tables…172
Static tables (lists)…172

Appendix B: Object.C Properties in VPN-1/FireWall-1 4.0

The Properties section of the $FWDIR/conf/objects.C file…177

Appendix C: Log Viewer "info" Messages

Messages in the 'info' column of the log viewer…190
More Information…192

Preface

Scope

The FireWall-1 Advanced Technical Reference Guide is intended to help the System Administrators:

1. Resolve common problems
2. Implement complex features

The guide was put together by the Check Point Escalation Support team, and makes available some of their real-world experience in assisting customers. Every chapter was written by a specialist in the field.

This guide does not duplicate the User Guides or Courseware. It either covers those topics not found in the User Guides, or expands on them.

This version of the Advanced Technical Reference Guide covers VPN-1/FireWall-1, and is updated to VPN-1/FireWall-1 4.1 SP1 (Check Point 2000), unless noted otherwise. Note that the previous version was called the "Advanced Troubleshooting Guide".

Links to SecureKnowledge and Other Places

You will get the most out of this guide if you use it on-line, while connected to the Internet. This is because the guide contains many links to solutions in the Check Point SecureKnowledge database http://support.checkpoint.com/kb/index.html.

SecureKnowledge is a self-service database of technical information to help you diagnose and solve installation, configuration, and upgrade problems with Check Point Software products.

To use SecureKnowledge you must be authenticated using your Support username and password. If you are not already authenticated, you will be required to do so the first time you click a link.

Who should use this Guide

This Troubleshooting Guide is written for people who provide Technical Support to System Administrators maintaining network security and Virtual Private Networks.

It assumes:

- A basic understanding and a working knowledge of VPN-1/FireWall-1
- Familiarity with the relevant User Guides

How to obtain the latest version of this Guide

The latest version of this guide can be found at http://www.checkpoint.com/support/technical/documents/

This guide is freely available to anyone who is registered to the (password protected) Check Point Technical Services Premium Support site http://www.checkpoint.com/support/technical/index.html.

Feedback Please!

We in Check Point Support would love to hear what you think of this guide. Please write to ehareven@checkpoint.com

Is the information is this guide useful?

Did you find what you were looking for?

What would you like to see in this guide?

Is there too much detail or not enough?

Summary of Contents

The Advanced Technical Reference Guide contains the following chapters. See the “Contents” for a summary:

Contents

Preface

Chapter 1: Troubleshooting Overview

Chapter 2: Troubleshooting Tools

Chapter 3: Troubleshooting Network Address Translation

Chapter 4: Troubleshooting Routers and Embedded Systems

Chapter 5: Troubleshooting Open Security Extension

Chapter 6: Troubleshooting Anti-Spoofing

Chapter 7: Troubleshooting Security Servers and Content Security

Chapter 8: Troubleshooting LDAP Servers and the AMC

Chapter 9: Troubleshooting Active Network Management

Chapter 10: Troubleshooting SNMP

Chapter 11: Troubleshooting Licensing

Chapter 12: What To Send Technical Support

Chapter 13: Check Point Support Information

Appendix A: State Tables for VPN-1/FireWall-1 4.0

Appendix B: Object.C Properties in VPN-1/FireWall-1 4.0

Appendix C: Log Viewer "info" Messages

Chapter 1: Troubleshooting Overview

Troubleshooting VPN-1/FireWall-1 issues can be very complex. Problems can be caused by network topologies, platform issues and the wide range of VPN-1/FireWall-1 features. Efficient troubleshooting must start with a carefully organized plan.

Troubleshooting Guidelines

1. **Define the problem as a list of symptoms.**

   Every problem can be described as a collection of symptoms. The first step is to define these symptoms.

   Possible symptoms are error and log messages, malfunctions of certain modules and user complaints.

2. **Make sure you have as much related information as you can.**

   Collect the log messages, error messages, and other symptom descriptions. Collect related information from product User Guides, release notes and any other source.

   Verify that the modules involved are correctly configured.

3. **Find a list of causes to every symptom.**

   Using the gathered information, try to find as many potential causes as you can for every symptom.

   Put the most likely cause first on the list and organize the rest in the same way.

4. **Start checking the causes one by one.**

   Make sure you initialize your environment setting before every test. Go from the most likely cause to the less.

5. **Consult other reference sources**

   Release notes, web sites, mailing lists, and Support. All these can be reached from the Check Point Premium Support site at http://www.checkpoint.com/support/technical/ (password required).

Information to Gather

Before contacting Technical Support, gather all necessary information about the problem. For a description of the of required information, Refer to

- “Chapter 12: What To Send Technical Support,” page 126
- “Contacting Check Point Worldwide Technical Services by Telephone,” page 133 and “Contacting Check Point Worldwide Technical Services by E-mail,” page 135

Chapter 2: Troubleshooting Tools

In This Chapter:

fwinfo 6

Introduction 6
How to create fwinfo 6
How to use the fwinfo output file 7
Sanity check 7
Extracting information from fwinfo.uue (UNIX only) 7

VPN-1/FireWall-1 Control Commands 8

fw ctl 8
Syntax 8
Explanation 8
fw ctl pstat 9
fw ctl debug 10
Syntax 10
The available fw ctl debug commands 10

FireWall-1 Monitor Command 16

Syntax 16
Options 17
Examples 17
Files 18
Notes 18

Debugging with INSPECT 19

Changing the log format 19
Using the debug command 20

More Information 20

Troubleshooting Tools

This chapter describes the most important tools for Troubleshooting VPN-1/FireWall-1 problems. These tools include `fwinfo`, Control (`fw ctl`) commands, the Monitor (`fw monitor`) Command and debugging with INSPECT.

fwinfo

Introduction

`fwinfo` is used to collect information that is used for debugging and solving VPN-1/FireWall-1 problems. It runs operating system and VPN-1/FireWall-1 commands and gathers information on the system parameters of the machine on which VPN-1/FireWall-1 is installed, and on VPN-1/FireWall-1 parameters such as interfaces and tables. The resulting file will usually be sent to Check Point Support (support@ts.checkpoint.com) for analysis.

How to create fwinfo

On NT

Issue the command:
`fwinfo >` `file_name`

The resulting file `file_name` will be uncompressed and not decoded. You should compress it before sending it to Check Point Support for analysis. Use any zip utility such as gzip, pkzip or winzip.

On UNIX

1. Before running `fwinfo`, make sure that the result of the `echo $FWDIR` command is `/etc/fw` (normally the FireWall directory). If it isn't, type
   `setenv FWDIR /etc/fw`
2. Login as a super user (recommended)
3. Run the script

   `$FWDIR/bin/fwinfo | compress | uuencode fwinfo.Z > /tmp/fwinfo.uue`

   which will do the following:

   (1) Run the fwinfo script (the directory will be `tar` compressed to `fwinfo.tar`, then

   (2) gzip the file to `fw.tar.gz`, then

   (3) uuencode it to fwinfo, then

   (4) Compress it under the original file name `fwinfo.Z`, then

   (5) The file will be uuencoded

The result is the file `/temp/fwinfo.uue`

How to use the fwinfo output file

The fwinfo file contains a lot of information. It is intended mainly for analysis by Check Point Support. However you can use it to solve problems by examining the file contents yourself. You will probably find only a small portion of it to be useful.

The information may be roughly divided into the following categories:

- General system data
- Network data
- FireWall-1 related data

Sanity check

You should begin by checking the most obvious points about the VPN-1/FireWall-1 and system configuration

System

To verify that the VPN-1/FireWall-1 is install on a supported system, look for the section `System Information`.

On Windows, the information is given in a straight-forward manner. e.g. Windows NT Version 4.0 (Service Pack 5 , Build:1381).

On a UNIX, the system information is given by the `uname -a`, and the output format varies slightly according to the exact UNIX flavor:

Table 1: UNIX system information obtained by issuing the command `uname -a`

OS	Format
AIX	AIX hostname OS-release OS-version machine-id
	(e.g. `AIX havitush 2 4 003831754C00`)
HPUX	HP-UX hostname OS-release OS-version HW/model machine-id license-level
	(e.g. `HP-UX drake B.10.20 A 9000/778 2007953537 two-user license`)
Solaris	SunOS hostname OS-release OS-version HW-name processor HW-platform
	(e.g. `SunOS bill 5.6 Generic_105181-05 sun4u sparc SUNW,Ultra-5_10`)
Linux	SunOS hostname OS-release OS-version HW
	(e.g. `Linux diana.checkpoint.com 2.2.5-15 #1 Mon Apr 19 22:21:09 EDT 1999 i586 unknown`)

Extracting information from fwinfo.uue (UNIX only)

Do the following:

	Run	To get
1	`uudecode fwinfo.uue`	`fwinfo.Z`
2	`uncompress fwinfo.Z`	`fwinfo`
3	`uudecode fwinfo`	`fw.tar.gz`
4	`gunzip fw.tar.gz`	`fw.tar`
5	`tar xvf fw.tar`	The directories: `conf/`, `lib/`, `state/`, `database/`, `log/`

VPN-1/FireWall-1 Control Commands

fw ctl

`fw ctl` commands send control information to the VPN/FireWall Kernel module.

This syntax and explanation is based on the VPN-1/FireWall-1 Administration Guide (version 4.0) or the VPN-1/FireWall-1 Reference Guide (version 4.1 and Check Point 2000).

This section focuses on the understanding the displayed VPN-1/FireWall-1 internal statistics, and the debug options of the `fw ctl` commands.

Syntax

```
fw ctl [ip_forwarding option] | Iflist | pstat | install | uninstall arp
```

Explanation

The commands are:

Command	Meaning

`ip_forwarding option`	`Option` is one of the following;
	`always`
	IP forwarding is active if and only if VPN-1/FireWall-1 is active, regardless of machine settings
	`never`
	IP forwarding depends on machine settings in /dev/ip, regardless of whether the FireWall is running or not
	`default`
	IP forwarding is active if the machine settings specify so, or if VPN-1/FireWall-1 is active

`pstat`	This command prints detailed information about the hash kernel memory in use (controlled by the parameter fwhmem) and the system kernel memory in use, including peak values of both. See fw ctl pstat, on page 9,
`iflist`	Prints the interface list as seen by the FireWall, for example: 0 : lo0 1 : en0 2 : en1
`install`	Installs the kernel module
`uninstall`	Uninstalls the kernel module
`arp`	Displays the ARP proxy table which is a mapping of IP and MAC addresses, and utilizes `local.arp` file
`debug`	A powerful VPN-1/FireWall-1debugging tool. With its many commands it is possible to see nearly everything that happens in the kernel module. See fw ctl debug on page 10

fw ctl pstat

The following is an explanation of some typical output from the `fw ctl pstat` command, which generates internal statistics. It prints detailed information about the hash kernel memory in use (controlled by the parameter `fwhmem`) and the system kernel memory in use, including peak values of both.

Output	`Hash kernel memory (hmem) statistics:`
	`Total memory allocated: 4194304 bytes in 1023 4KB blocks using 1 pool`
	`Total memory bytes used: 201600 unused: 3992704 (95%) peak: 205872`
	`Total memory blocks used: 53 unused: 970 (94%)`
	`Allocations: 61671 alloc, 0 failed alloc, 59509 free`

Explanation	A pool of 4194304 bytes was allocated by the VPN/FireWall module kernel for its internal hash table items and other kernel data structures. 3992704 bytes are available in that pool. There are 61671 allocation operations and 59509 free operations while none had to be rejected due to memory exhaustion.

Output	`System kernel memory (kmem) statistics:`
	`System physical memory: 62857216 bytes`
	`Available physical memory: 3072000 bytes`
	`Total memory bytes used: 5615497 peak: 5712425`
	`Allocations: 552 alloc, 0 failed alloc, 254 free, 0 failed free`

Explanation	The amount of system physical memory is 62857216 bytes while 3072000 bytes are available for kernel allocation (note that this information is not display on all supported platforms). 5615497 bytes of kernel memory are used by the Firewall kernel module (including that hash memory) and the peak usage was 5712425 bytes.
Output	`Inspct: 1853775 packets, 215915927 operations, 5098022 lookups, 241118 record, 94958150 extract`
Explanation	This information relates to the activity of the virtual machine. (The figures relate to virtual machine operations, lookups and records in tables, and the number of packets inspected).
Output	`Cookies: 1972405 total, 411870 alloc, 411870 free, 30001 dup, 4344704 get, 120861 put, 2038056 len`
Explanation	FireWall-1 uses an abstract data type (cookie) to represent packets. These statistics relate to the code that handle those cookies and is used only for heuristic tuning of the code.
Output	`Fragments: 142389 fragments, 0 expired, 24012 packets`
Explanation	FireWall-1 performs 'virtual reassembly' which means that it gathers all the fragments of a packet before processing that packet. This statistics information tells us that the kernel module has processed 142389 fragments and assembled them to 24012 packets while non fragment were expired. Fragments expire when their packet fails to be reassembled in a 20 seconds time frame or when due to memory exhaustion, they cannot be kept in memory anymore.
Output	Encryption: 39948 encryption, 38797 decryption, 22348 short, 0 failures.
Explanation	This information relates to number of encrypted/decrypted packets encrypted by the kernel). The 'short' element refers to the number of packets which were not encrypted due to the fact that they had no data in them (they had only headers, and the fwz scheme does not encrypt headers).
Output	Translation: 245/1023021 forw, 222/829627 bckw, 467 tcpudp, 0 icmp, 36-31 alloc .
Explanation	This information relates to address translation. 245 of the 1023021 packets, going in the 'forward' direction (forward – outgoing, backward - incoming), while 222 of the 829627 packets, going on the 'backward' direction, were translated. 467 of the translations were of tcp/udp packets while no ICMP packet had to be translated. 36 tcp/udp port numbers where dynamically allocated while 31 where de-allocated.

fw ctl debug

The `fw ctl debug` command is a powerful debugging tool, which is very helpful when debugging VPN-1/FireWall-1.

With its many commands it is possible to see nearly everything that happens in the kernel module.

Syntax

```
fw ctl | all | cookie | crypt | driver | filter | hold | if | ioctl | kbuf
| ld | log | machine | memory | misc | packet | q | tcpseq | xlate, xltrc
| winnt | synatk | domain | install | profile | media | align | ex |
balance | chain
```

To start debug mode;

```
fw ctl debug [command]
```

To cancel the debugging;

```
fw ctl debug 0
```

Apart from this method of operation there is an option to use the debug commands from a window rather than from the console (console being the default option).

In most cases, you would need to run the debug as follows:

```
% fw ctl debug –buf [buffer size] /* direct the information to a buffer */
% fw ctl debug command1 command2  /* generate the required data in that buffer */
% fw ctl kdebug –f > output_file  /* Read the kernel buffer and print it to a file */
```

After all the necessary data is gathered, interrupt the last command using `Ctrl-C`

Cancel the debugging using `fw ctl debug 0`

The available fw ctl debug commands

Option	Meaning
all	All the switches. This option is not recommended. The amount of data massive and it will be almost impossible to get any useful information. On some platforms it could crash the machine, as the operating system will try to write massive amounts of data to the console.

Cookie	With the cookie switch turned on, all the cookies (the data structure that holds the packets) are shown. (cookies are used in order to avoid the problems that arise from the ways different Operating Systems handle packets).
	
	Example:
	`M_dup(fwcookie.c:2464): 7E492D0`
	`m_dup(fwcookie.c:2464): 7E492D0`
	
	Explanation
	Those are just pointers to the data. (the actual cookies)

crypt	With this option turned on, all the encrypted/decrypted packets are printed in clear text and cipher text. The algorithms and keys that used are also printed See “crypt” Example, Output and Explanation, on page 12.

Option	Meaning

driver	Access to the kernel module is shown (log entries).
	Example Output
	`fw_read: non blocking read returns`
	`fw_read: log_first = 1276, len = 36`
	`fw_read: log_first = 1316, len = 36`
	`fw_read: log_first = 1356, len = 52`
	Explanation:
	Those are kernel calls about log entries read.

filter	Shows the packet filtering that is done by the kernel module, and all the data that is loaded into the kernel (the building of the tables, the services and the filtering functions.)
hold	This is the holding mechanism and all packets that are being held or released are shown when this switch is turned on (for example when doing encryption).
if	All the interface related information (accessing the interface, installing on interface).
ioctl	When this switch is turned on it shows all the `ioctl` (I/O control) messages such as the communication between the kernel and the daemon, loading and unloading of VPN-1/FireWall-1. (For instance when the daemon exits, it is sometimes possible to see the `ioctl` command that caused the exit.)
kbuf	All the information that is kbuf related (such as rdp when encrypting). The kbuf is the kernel buffer memory pool, and the encryption keys use these memory allocations. (The memory switch is for the tables memory pool).
Ld	All the reads and writes to the tables. (heavy)
Log	This switch shows everything related to the log (all log calls).
Machine	This switch shows the actual assembler commands that are being processed. (heavy)
memory	The memory allocations of VPN-1/FireWall-1.
Misc	All the things that are not shown with the other commands.
Packet	This switch shows all the actions performed on a packet (accept, drop, fragment).
Q	The information regarding the driver queue (streams queues operations).
tcpseq	This switch prints the tcp sequences that are being changed when using address translation.
xlate, xltrc	Prints the NAT related information (changing IPs…) where the xlate switch is the basic (and most commonly used) switch, and xltrc gives additional information by showing the actual process of going through the NAT Rule Base for each packet (mostly on telnet and ftp). See xlate, xltrc on page 14.
Winnt	Special information regarding the Windows NT operation.
synatk	All the information regarding the Syndefender.
domain	Domain queries.
Install	Driver installation.
Profile	Prints the number of packets that were filtered and the amount of time spent on them.
Media	Make level info on NT (frames and not packets).
Align	Gives information regarding the decoding of the H323 data in H323 data connections.
Ex	Information about dynamic table expiration.
Balance	Information about load balancing.
Chain	Information about cookie chains.

crypt

With this option turned on, all the encrypted/decrypted packets are printed in clear text and cipher text. The algorithms and keys that used are also printed

Example	**Encrypting ICMP with fwz1 using SecuRemote.** **(The line numbers are not shown in the actual debugging and have been added for convenience).**
Output	1. fw_crypt: op=decrypt method=0 md=1 entry=4 len=60 offset=24 2. fw_crypt: cookie=7E492D0, cookie_m=5A49600, packetid=9E00 3. fw_crypt: keybuf=7E86290 keylen=6 keyval=(1E,42,8A,D2,2,52) 4. fw_crypt: mdkeylen=32 mdkey=(61,8F,DF,A4,AB,7C,AA,5E,96,F,53,36,1C,92,B1,47,55,C8,1F,8B,6A, DE,CB,62,65, FB,51,52,6B,63,4,C2) 5. fw_crypt: niv=4 iv=(E7,A,8,0) 6. fw_crypt: crunched iv=(E7,A,8,0,E7,A) 7. fw_crypt: just before calling fwcrypto_do() 8. cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0 9. 0: 45 00 00 3C E7 0A 00 00 20 01 76 1F C0 A8 6E 05 16: C7 CB 47 1E 08 00 F9 5B CF 8D F1 86 98 28 92 87 32: A8 7F 80 4F 79 C4 0E 4F 3B 72 CA 32 4E CB A6 96 48: 45 95 D1 A3 15 11 76 07 C4 42 1C 2B 10. fw_crypt_check_md: mdlen=16 md=(B1,8B,69,CA,62,FE,AB,67,79,27,88,55,15,14,7F,B4) 11. fw_crypt: just after calling cookie_put_data() 12. cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0 13. 0: 45 00 00 3C E7 0A 00 00 20 01 76 1F C0 A8 6E 05 16: C7 CB 47 1E 08 00 F9 5B 02 00 52 00 61 62 63 64 32: 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 48: 75 76 77 61 62 63 64 65 66 67 68 69
Explanation	1. op=decrypt – the operation that is being done now is decryption. method=0 – the method is fwz1 (this is vesion specificand in this case it is the vpn version). md=1 – using MD5. Entry=4 – entry number is 4 (in the connection table this means responder of encrypted connection - see“connections table,” page 142, in the Tables section). Len=60 – packets length is 60. offset=24 – start decrypting after 24 bytes (the first 24 bytes are the IP header and part of the ICMP header as well) 2. cookie=7E492D0, cookie_m=5A49600 – where the data is actually being stored (pointers). packetid=9E00 – the packet id of this packet (in VPN-1/FireWall-1 each packet has a unique packet id that is used to identify the packet for further use such in the “hold” table.) 3. keybuf=7E86290 – pointer to encryption key. keylen=6 – the length of the key is 6 bytes. keyval=(1E,42,8A,D2,2,52) – the actual data encryption key (6 bytes) 4. mdkeylen=32 – the length for the MD5 key is 32 bytes (the data authentication key). mdkey=(61,8F,DF,A4,AB,7C,AA,5E,96,F,53,36,1C,92,B1,47,55,C8,1F,8B,6A,DE,CB,62,65,FB,51,52,6B,63,4,C2) - the actual MD5 key (32 bytes) 5. niv=4 iv=(E7,A,8,0) – niv and iv are parameters of the Initialization Vector used to generate the encryption key 6. crunched iv=(E7,A,8,0,E7,A) – a manipulation of the IV that is used for the actual key calculation 7. just before calling fwcrypto_do() - a debugging line that says that the actual function that will do the decryption is about to be called. 8. cookie 0x7E492D0: m=0x5A49600, - the pointers to the data, offset=0, - the offset of IP in link layer datagram, len=60, - the data length (60 bytes) flen=0 – number of bytes in the first block of data.

	9. The actual data in the packet still encrypted (the first 20 is header, then 8 ICMP header, the rest is the actual data in this packet - ICMP echo request). 10. mdlen=16 – the MD5 checksum length is 16. md=(B1,8B,69,CA,62,FE,AB,67,79,27,88,55,15,14,7F,B4) the actual MD5 hash - no errors are reported meaning the data integrity is not compromised. 11. fw_crypt: just after calling cookie_put_data() – a debugging line that shows that the decrypted data was returned to the cookie 12. cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0 - the data cookies (see line 8). 13. The actual data in clear text, you can compare and see that the first 24 bytes in the packets on lines 9 and 13 are the same, those are the headers which are not encrypted, the next 4 are control characters which are encrypted and afterwards the actual data which on the second packet (line 13) is sequential as it should be in ICMP and on the encrypted packet it is garbled.

Output	1. `fw_crypt_make_md: mdlen=16`
	`md=(5D,44,68,66,CC,68,78,D5,3C,1F,31,A2,50,86,CF,5C)`
	2. `fw_crypt: op=encrypt method=0 md=1 entry=3 len=60 offset=24`
	3. `fw_crypt: cookie=7E492D0, cookie_m=5A49600, packetid=9E01`
	4. `fw_crypt: keybuf=7E86210 keylen=6 keyval=(1E,42,8A,D2,2,52)`
	5. `fw_crypt: mdkeylen=32`
	`mdkey=(61,8F,DF,A4,AB,7C,AA,5E,96,F,53,36,1C,92,B1,47,55,C8,1F,8B,6A,DE,CB,62,65,FB,51,52,6B,63,4,C2)`
	6. `fw_crypt: niv=4 iv=(1C,4,0,0)`
	7. `fw_crypt: crunched iv=(1C,4,0,0,1C,4)`
	8. `fw_crypt: just before calling fwcrypto_do()`
	9. `cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0`
	10.. `0: 45 00 00 3C 1C 04 00 00 FF 01 62 25 C7 CB 47 1E`
	`16: C0 A8 6E 05 00 00 01 5C 02 00 52 00 61 62 63 64`
	`32: 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74`
	`48: 75 76 77 61 62 63 64 65 66 67 68 69`
	11. `fw_crypt: just after calling cookie_put_data()`
	12. `cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0`
	13. `0: 45 00 00 3C 1C 04 00 00 FF 01 62 25 C7 CB 47 1E`
	`16: C0 A8 6E 05 00 00 01 5C 61 EB 75 99 12 89 96 AB`
	`32: 80 D8 C2 7B 45 75 FD D6 E9 6E 95 01 31 E8 59 3E`
	`48: FF B6 7D 62 D0 2D 2E 87 A6 6D 84 A9`

Explanation	1. mdlen=16 – length of the MD5 checksum is 16 byte md=(5D,44,68,66,CC,68,78,D5,3C,1F,31,A2,50,86,CF,5C) - the actual MD5 hash 2. op=encrypt - the operation is encryption. Method=0 - using fwz1 (this is version specific and in this case it is the VPN version) md=1 - using MD5 data integrity. entry=3 - a certain entry in the connection table will have a value of 3 meaning it is an initiator of an encrypted connection (see connection table). len=60 - the packet length is 60 bytes. offset=24 – the decryption will start after 24 bytes (the first 24 bytes are IP and part of the CMP header). 3. Cookie=7E492D0, cookie_m=5A49600, - the cookies are the pointers to the actual data. Packetid=9E01 - the packet id is greater by one from the previous packet (see line 2 in the initial information section above). 4. Keybuf=7E86210 - pointer to the encryption key. keylen=6 - the length of the data encryption key (in bytes). Keyval=(1E,42,8A,D2,2,52) - the actual data encryption key. 5. Mdkeylen=32 – the length of the MD5 key is 32 byte. Mdkey=(61,8F,DF,A4,AB,7C,AA,5E,96,F,53,36,1C,92,B1,47,55,C8,1F,8B,6A,DE,CB,62,65,FB

	,51,52,6B,63,4,C2) - the actual MD5 key. 6. niv=4 iv=(1C,4,0,0) - the initialization vector used in the process of calculating the data encryption key. 7. Crunched iv=(1C,4,0,0,1C,4) – the actual initial vector that is used in the data encryption key calculation. 8. just before calling fwcrypto_do() - a debugging line that says that the actual function that does the encryption is about to be called. 9. Cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0 - the cookies that hold the data (see line 8 on previous section) 10. the actual packet data before the encryption (in clear text). 11. fw_crypt: just after calling cookie_put_data() - a debugging line that shows that the encrypted data was just returned to the cookie. 12. Cookie 0x7E492D0: m=0x5A49600, offset=0, len=60, flen=0 - see line 9 13. the actual encrypted data.

xlate, xltrc

Prints the NAT related information (changing IP addresses etc.) where the `xlate` switch is the basic (and most commonly used) switch, and `xltrc` gives additional information by showing the actual process of going through the NAT Rule Base for each packet (mostly on TELNET and FTP).

Example	Translating ICMP using the hide method (xlate command).
Output	1. `fw_xlate_icmp: got backw connection src C0A86E05 dst C25A0105 type 8 code 0 id F00E` 2. `fw_xlate_icmp: got backw icmp request (8)` 3. `fw_xlate_icmp: got forw connection src C0A86E05 dst C25A0105 type 8 code 0 id F00E` 4. `fw_xlate_match_entry: connection matches` 5. `fw_init_xlation: src=C0A86E05 sport=200 dst=C25A0105 dport=2E00 ip_p=1 mthd=1` 6. `allocate_port: addr=C7CB471E, first=258, last=3FF, start=283, old_port=200` 7. `allocate_port: found a free port <C7CB471E,1,284>` 8. `fw_init_xlation_tables: adding <C0A86E05,200,C25A0105,2E00,1;C7CB471E,80000284,C25A0105,2E00,0/30> to forw` 9. `fw_init_xlation_tables: adding <C25A0105,2E00,C7CB471E,284,1;C25A0105,2E00,C0A86E05,80000200,0> to backw.` 10. `fw_xlate_icmp: changing packet's src,dst to <C7CB471E,C25A0105>` 11. `fw_xlate_icmp: got backw connection src C25A0105 dst C7CB471E type 0 code 0 id 7683` 12. `fw_xlate_icmp: got (C25A0105,2E00,C0A86E05,80000200) from fwx_backw_tab` 13. `fw_xlate_deallocate: hval = C0A86E05,200,C25A0105,2E00,1;C7CB471E,80000284,C25A0105,2E00,0` 14. `deallocate_port: port is marked` 15. `deallocate_port: attempting free port 284 (protocol 1) of host C7CB471E` 16. `fw_xlate_deallocate: deleting <C25A0105,2E00,C7CB471E,284,1> from fwx_backw_tab` 17. `fw_xlate_icmp: changing packet's src,dst to <C25A0105,C0A86E05>` 18. `fw_xlate_icmp: got forw connection src C25A0105 dst C0A86E05 type 0 code 0 id 7683` 19. `fw_xlate_icmp: got forw icmp reply (0)`

Explanation	1. VPN-1/FireWall-1 receives a back connection type 8 code 0 2. The request is ICMP echo request (type 8) 3. VPN-1/FireWall-1 understands that the connection must be an outgoing connection (type 8 is echo request and not echo reply). 4. The connection matches the rule base 5. src=C0A86E05 sport=200 dst=C25A0105 dport=2E00 ip_p=1 mthd=1 - the xlation is initiated, the connection is written, - src – source IP (hex), sport – source port, dst – destination IP, ip_p - IP protocol 1=ICMP, mthd – method - 1 = hide (see tables section, xlate tables) 6. VPN-1/FireWall-1 is trying to allocate a port for the translation, the entry is the allocation table (see tables, in this case (ICMP) the port is a sequential number) 7. VPN-1/FireWall-1 has found a port, the entry is ip_address,method, new_port 8. Adding the connection to the “fwx_forw table,” (page 150) 9. Adding the connection to the table “fwx_backw table,” (page 150) 10. The actual translation, the source and the destination of the packet is changed. 11. A backw connection has arrived type 0 code 0 (ICMP echo reply) 12. The arriving connection matches an existing connection in the “fwx_backw table,” (page 150) 13. The connection is complete and marked for delete 14. The port is marked to be freed 15. The allocated port is de allocated 16. The connection is deleted from the fwx_backw table,” (page 150) table. 17. The arriving packet is translated according to the table as “fwx_backw table,” (page 150) connection. 18. VPN-1/FireWall-1 finishes the connection, the connection is printed 19. The connection is marked a being an ICMP echo reply (code 0).

FireWall-1 Monitor Command

The **`fw monitor`** command can be used to monitor network traffic through the FireWall. This is done by loading a special INSPECT filter (separate from the one that is used to implement the security policy) that is used to filter out interesting packets which are then displayed to the user.

Syntax

```
fw monitor [-d] [-D] <{-e expr}+|-f <filter-file|->> [-l len] [-m mask] [-
x offset[,len]] [-o <file>]
```

The filter can be specified from a file (`-f` option) or from the command line (`-e` option).

There are 4 inspection points along the passage of a packet through VPN-1/FireWall-1:

- Before the virtual machine in the inbound direction (i or PREIN)
- After the virtual machine in the inbound direction (I or POSTIN)
- Before the virtual machine in the outbound direction (o or PREOUT)
- After the virtual machine in the outbound direction (O or POSTOUT)

The term virtual machine above refers to most of the packet processing done by the FireWall and not only to the INSPECT code execution (including virtual defragmentation, NAT, encryption, etc.).

Once started the command will compile the specified INSPECT filter program, load it to the kernel (not replacing the security policy), and then the program will continuously get packets from the kernel and display them in the terminal window (from which the command was issued). Upon an interrupt signal (Control-C) or other catchable signal, the program will stop displaying packets, unload the monitor filter and exit.

The INSPECT program which is used to filter the monitored packets should return accept in order for the packet to be displayed, any other return code from INSPECT (or the implicit drop at the end) will cause the packet not to be displayed. No scoping should be used in the filter program (e.g. => le0@all...), since the same filter is executed in all interfaces and in all directions. Instead, an expression such as direction=0,ifid=1, should be used (the interface id number for an interface can be found by using the `fw ctl iflist` command). Tables and functions can be used, care should be taken though, not to use table names that are used by the security policy.

Unless the `-o` option was specified, packets are displayed to the standard output (control messages are printed on the standard error), the first line will display IP information, the next lines will display protocol specific information (for TCP, UDP or ICMP). If the display option (`-x`) is used the following lines will show a hex dump and printable character display of the packet content.

Packets are inspected in all 4 points mentioned above unless a mask is specified (`-m` option).

Options

Switch:	Explanation:
`-d`	Provides lower level debug output from the filter loading process
`-D`	Provides higher level debug output from the filter loading process
`-e`	Specify an INSPECT program line (multiple -e options can be used) .
`-f`	Specify an INSPECT filter file name ('-' means the standard input), the file is copied before compilation. The -f and -e options are mutually exclusive.
`-l`	Specify how much of the packet should be transferred from the kernel (for packets longer than the specified length only a prefix will be available for display).
`-m`	Specify inspection points mask, any one or more of i, I, o, or O can be used (the meaning of each is explained above).
`-o`	Specify an output file. Save 'monitored' packets in the output file as they are monitored. During the monitoring, a count of the number of packets saved in the file is displayed. The content of the file can later be examined by the snoop -i <file> command.
`-x`	Specify display parameters. When this option is present, the IP and protocol information will be followed by a hex dump and printable character display, starting at the offset bytes into the packet for len bytes long. (If offset + len is larger than the length specified by the -l option, only the data available will be displayed).

Examples

`fw monitor -e '[9:1]=6,accept;' -l 100 -m iO -x 20`

This will display all TCP packets going through the FireWall, once before the virtual machine in the inbound direction and once after the virtual machine in the outbound direction (provided, of course, that the FireWall allowed the packet to pass). Up to 80 bytes of the TCP header and data will be displayed (assuming no IP options).

`fw monitor -e 'accept;' -m iI -o /tmp/monitor.snp`

`<ctrl-c>`

`snoop -i /tmp/monitor.snp -V -x14  tcp port ftp or tcp port ftp-data`

This will save all packets going into the FireWall, one before the virtual machine in the inbound direction and once after the virtual machine in the inbound direction, in the file `/tmp/monitor.snp`. This file should later be copied to a Solaris machine and can be examined by the snoop utility. In the previous example, display only TCP packet going from or to the ftp or ftp-data port.

Alert - 19 Dec 1999 **-** A security hole has been discovered in the "snoop" application that could allow a malicious user to gain privileged access to a machine running "snoop".

Sun Microsystems has provided patches to fix this security hole. They can be downloaded from:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches

Sun has issued a Security Bulletin #00190 regarding this vulnerability. See http://sunsolve.sun.com/pub-cgi/secBulletin.pl

Since "snoop" presents a security risk, Check Point recommends that running snoop should be avoided. `fw monitor` should be used instead, which will usually provide more information than

snoop. Where snoop is the only way to obtain information, verify that the Sun patches have been applied before running the snoop.

Files

Filename:	Explanation:
`$FWDIR/tmp/monitorfilter.pf`	The (copied) INSPECT filter file.
`$FWDIR/tmp/monitorfilter.*` (`.*` for `.fc`, `.ft`, etc.)	Output files of the compilation. These are removed before the program exits.

Notes

It is extremely important to avoid interfering with the security policy tables, or unexpected behavior may result (which may include a machine crash). In the "post machine" inspection points (I and O) packets are "defragmented", which means that the packet data buffer transferred from the kernel includes data from all IP fragments, but only the IP header of the first fragment (which indicates the length of the first fragment only). An exception to this is, for example, when there is no virtual defragmentation (such as when no security policy is loaded on the FireWall).

Any load, fetch or unload of the security policy while `fw monitor` is running will cause the monitor filter to be unloaded and the program to exit.

Debugging with INSPECT

Important: Check Point will not support customer changes to the Inspect code.

There are two main ways of using the INSPECT language to debug the Security policy:

1. **Changing the log format** in order to display additional information about packets going through the FireWall.
2. **Inserting debug lines in the INSPECT code** to show run time information and to check where the code is entered.

Changing the log format

The two most important files that are needed in order to modify the log format are: `formats.def` and `fwui_head.def`

The log formats appear in `formats.def` in Short and Long formats, and contain information that is relevant to the protocols and VPN-1/FireWall-1 features used in the rule. For instance, there is a different format for ICMP long log format, and long log formats for other protocols.

In order to display additional information in an existing log format, add a line to the format with the following model:

```
<”information_label”, information_type, information_value>,
```

Example: To add the packet length to the short format (it already exits in the long format).

The packet length is defined as `ip_len` in `tcpip.def` where the definitions of the header fields in IP, TCP, UDP, ICMP,… protocols can be found.

The original format is:

```
short = format {
      <"proto", proto, ip_p>,
      <"src", ipaddr, src>,
      <"dst", ipaddr, dst>,
      <"service", port, dport>
};
```

It must be modified to:

```
short = format {
      <"proto", proto, ip_p>,
      <"src", ipaddr, src>,
      <"dst", ipaddr, dst>,
      <"service", port, dport>,
      <"length", int, ip_len>       /* ---> added line <---  */
};
```

The new field will be added to the Info column in the Log Viewer (see “Appendix C: Log Viewer "info" Messages,” page 189.

Using the debug command

The debug command makes it possible to see which part of the code is entered and when.

Insert a debug command at the end of the condition that you want to test. In the following example, we want to see when the test for an ftp connection is verified and to know what was the source (`Ip_Src` is defined in `tcpip.def`) of the packet.

```
eitherbound all@ariel
      accept      start_rule_code(1),
            (tcp, ftp),
            RECORD_CONN(1),
            LOG(short, LOG_NOALERT, 1),
            debug ip_src;  /* this is the line we inserted to get the
debug */
eitherbound all@ariel
      accept      start_rule_code(2),
            (tcp, http),
            RECORD_CONN(2),
            LOG(short, LOG_NOALERT, 2);
eitherbound all@ariel
      accept      start_rule_code(3),
            (tcp, telnet),
            RECORD_CONN(3),
            LOG(short, LOG_NOALERT, 3);
eitherbound all@ariel
      accept      start_rule_code(4),
            (icmp, icmp-proto),
            RECORD_CONN(4),
            LOG(short, LOG_NOALERT, 4);
eitherbound all@ariel
      accept      start_rule_code(5),
            RECORD_CONN(5);
            .
            .
            .
```

The debug command can be also inserted other INSPECT files, specifically the `.def` files, mainly `base.def` where are the definition of packet inspection for the different protocols.

Another format exists for debug. It is possible to print several data in one command by using:

`debug <number1,number2,number3,...>;`

Only numbers can be displayed because that is the only type known by INSPECT. They are printed in a hexadecimal form.

The new policy has to be loaded after the modification: `fw load <policy_file>`

Then write: `fw ctl debug –buf` to redirect the result of the debug command to a buffer, and

`fw ctl kdebug –f [> <filename>]` to send the results to the standard output or redirect the buffer to a file.

More Information

For more information on INSPECT and VPN-1/FireWall-1 Control (`fw ctl`) commands see the VPN-1/FireWall-1 4.1 and 4.1 SP1 (Check Point 2000) Reference Guides

Chapter 3: Troubleshooting Network Address Translation

In This Chapter:

Introduction 22

Resolving Common NAT Problems 22

Optimizing Network Performance with NAT 22
How to NAT (Network Address Translate) a DMZ host accessed by external hosts without applying the NAT on the internal network 22
How to set up Hide Mode Address Translation behind a dynamic address 23
How to use Encryption with NAT and ICMP 23
How to Connect several illegal IP networks through the Internet 23
Is there a limitation on XLATE_HIDE? 24
How to Configure SecuRemote with Split DNS for an Internal DNS Server 24
How to use NAT when the IP address is embedded in the data area 24
Does the ident service work with Hide NAT? 25
If the external IP address of the FireWall is an illegal address, can you connect to it via SecuRemote? 25
“Leaky” NAT 26
Cause 26
Troubleshooting 26
How to workaround this issue 26
1. Increase the TCP timeout value 26
2. Increase TCP timeout for a specific service 26
3. Increase the value out of the TCP start time out (tcpstarttimeout) parameter 26
4. Increase the value of the TCP end timeout (tcpendtimeout): 27
5. Change the relevant service to a service of type 'other' and not 'TCP': 27
6. Applying the ACK Denial-Of-Service hotfix. 27

Debugging NAT 28

More Information 28

Troubleshooting Network Address Translation

Introduction

Network Address Translation (NAT) involves replacing one IP address in a packet by another IP address. NAT is used in two cases:

1. The network administrator wishes to conceal IP addresses in the internal networks from the Internet
2. The IP addresses of the internal network use invalid Internet addresses. That is, as far as the Internet is concerned, these addresses belong to another network or use a private address range.

This chapter provides additional information about Address Translation that is not covered in the User Guides.

Resolving Common NAT Problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

Optimizing Network Performance with NAT

Access to State Tables is a major factor in the performance overhead of Network Address Translation (NAT). By increasing the limit and hash-size of these two tables, you may be able to improve the performance of the Address Translation– especially the “fwx_backw table,” page 150 and the “fwx_forw table,” page 150 in “Appendix A: State Tables for VPN-1/FireWall-1 4.0,”

The value of the hash-size should be a power of 2, such that the normal number of entries in that table is usually lower than 2*hashsize.

How to NAT (Network Address Translate) a DMZ host accessed by external hosts without applying the NAT on the internal network

Use the following Rule Base:

No	Source	Destination	Service	Source	Destination	Service
1	DMZ	DMZ	Any	=	=	=
2	InternalNetwork	InternalNetwork	Any	=	=	=
3	DMZ	InternalNetwork	Any	=	=	=
4	InternalNetwork	DMZ	Any	=	=	=
5	DMZ	Any	Any	DMZ-Static	=	=
6	InternalNetwork	Any	Any	InternalNetwork-Hide	=	=

Then the DMZ addresses will not be translated when going to the Internal Network, and translated otherwise. If the Internal Network is not translated, you can omit rules 2,4,6.

See the SecureKnowledge Solution (ID: 36.0.1738860.2502469) in the Check Point Technical Services site

How to set up Hide Mode Address Translation behind a dynamic address

To hide a range of address behind a dynamic IP address, hide the range behind the IP address 0.0.0.0. VPN-1/FireWall-1 will determine the exact IP of the hiding address as the address that the packets exit from.

1. Open the security policy editor.
2. Create a new workstation object for the network/address range being NATed.
3. Input the pertinent information on the general tab (name and IP).
4. Click on the NAT tab.
5. Click "use automatic translation rules".
6. Set the mode to "hide" and input 0.0.0.0 as the Hiding IP address.

Cause: An ISP did not provide a static IP address.

See the SecureKnowledge Solution (ID: 36.0.1738860.2502469) in the Check Point Technical Services site

How to use Encryption with NAT and ICMP

Problem Description: Cannot encrypt and do NAT simultaneously on ICMP packets

To enable this feature you should quit all control GUIs, both fwui and GUI-clients (Windows and Motif) and then manually edit the `'objects.C'` file (in `'$FWDIR/conf'` for UNIX, `'%SystemRoot%\fw\conf'` for NT). Change the line `":icmpcryptver (0)"` to `":icmpcryptver (1)"`. This change should be made in all encrypting/decrypting machines in your VPN

NOTE: Making the change disables the Backward Compatibility of encrypting ICMP packets, such as ping. This means that all affected machines will not be able to encrypt ICMP (with or without NAT) against VPN-1/FireWall-1 from versions earlier than 3.0, and version 3.0 FireWalls which did not make this modification.

It is only necessary to modify the `'objects.C'` file in the management stations. After modifying `'objects.C'`, reinstall the security policy on all VPN-1/FireWall-1 modules in the VPN. Once this modification is done, VPN machines should be able to use encryption and address translation with ping.

See the SecureKnowledge Solution (ID 36.0.2056964.2506360) in the Check Point Technical Services site

How to Connect several illegal IP networks through the Internet

Sometimes it is necessary to connect several networks with illegal addresses via the Internet. This is a problem, because a client can only access a computer on another network if it can reach the IP address of that network

One way to do this is to get legal IP addresses for the computers which need to be servers for the other networks. Then, use Static Address Translation to translate the addresses of the servers, and Hide Address Translation for everything else, so that the IP addresses will look like the following:

In Network	Source IP	Destination IP
Internal-1 (the client's net)	Client (illegal)	Server (legal)
Internet	Address client is hidden to, usually Internal-1's gateway (legal)	Server (legal)
Internal-2 (the server's net)	Address client is hidden to, usually Internal-1's gateway (legal)	Server (illegal)

Another possibility is to use IP tunneling, to tunnel the IP packets with illegal source and destination addresses in the data portion of legally addressed IP packets which pass between the gateways.

Note: The following instructions show how to change both the source and destination address in address translation rules. The procedure makes it possible to use the server's illegal IP address in the internal network by creating the following address translation rule:

1. Original Packet
   Source | Destination | Service
   Internal-1 network | Server's Illegal | any
2. Translated Packet
   Source | Destination | Service
   Internal-1's Gateway (hide) | Server's Legal | Original
3. Install on Internal-1's Gateway

In this case, the IP addresses will look like this:

In Network	Source IP	Destination IP
Internal-1 (the client's net)	Client (illegal)	Server (illegal)
Internet	Internal-1's gateway (legal)	Server (legal)
Internal-2 (the server's net)	Internal-1's gateway (legal)	Server (illegal)

Note: SKIP and IPSEC, which encapsulate the IP packets, do not require any of the above, and allow you to disregard the whole issue.

See the SecureKnowledge Solution (ID 36.0.2512318.2514147) in the Check Point Technical Services site

Is there a limitation on XLATE_HIDE?

There is no limit on the number of internal computers that use FW_XLATE_HIDE. However, there is a limit on the total number of address translated connections. The default size for the NAT tables is 25,000 and can be enlarged to 50,000.

See the SecureKnowledge Solution (ID 36.0.2437377.2512633) in the Check Point Technical Services site

How to Configure SecuRemote with Split DNS for an Internal DNS Server

Problem Description: DNS queries to the Internal Domain may be encrypted and resolved by the Internal DNS server

Refer to the document: “How to Configure SecuRemote with Split DNS for an Internal DNS Server”. (See the SecureKnowledge Solution (ID 55.0.790723.2565472) in the Check Point Technical Services site)

All DNS queries other than those to the Internal Domain are resolved by an external (ISP) public DNS server

The security aspect of Split DNS is clearly to hide internal domain information from the outside world

Split DNS can also prove valuable for non routable internal address schemes such as 10.x.x.x or 172.x.x.x

See the SecureKnowledge Solution (ID 55.0.790723.2565472) in the Check Point Technical Services site

How to use NAT when the IP address is embedded in the data area

There are certain protocols, such as the one used to communicate between a Primary Domain Controller and Backup Domain Controller in Windows, which put the IP address in the data area, where VPN-1/FireWall-1 doesn't know how to change it unless NAT has been adapted specifically to that protocol.

In these cases it is sometimes possible to use two VPN-1/FireWall-1 gateways with Address Translation to still allow the protocol to be used.

If there is a VPN/FireWall module on the client side of the Internet, as follows:

Server-------FW-1-------Internet---------FW-1 ---------Client

You can use DST Static Address Translation, which will translate the illegal IP address of the server to it's legal IP address.

For example, suppose that the server's illegal IP address is 10.0.0.1, and it's legal IP address is 197.3.5.10. In this case, you would have the following address translation rule on the FireWall at the exit of the server's LAN:

Source	Destination	Service	Source	Destination	Service
10.0.0.1	any	any	197.3.5.10(s)	any	any
Any	197.3.5.10	any	Any	10.0.0.1(s)	any

In this case you'd need the following rule on the FireWall on the client side:

Source	Destination	Service	Source	Destination	Service
Any	10.0.0.1	any	Any	197.3.5.10(s)	any
197.3.5.10	any	any	10.0.0.1(s)	any	any

Then, the packet will travel the Internet with the legal IP address of the server, but both the client and the server will see it with it's illegal address. Note that if the client's IP address is also illegal you would need to use dual Address Translation.

See the SecureKnowledge Solution (ID 36.0.2437410.2512633) in the Check Point Technical Services site

Does the ident service work with Hide NAT?

Ident is not reliably supported when attempting to get identification information for IP addresses which are used to FWXT_HIDE multiple computers.

See the SecureKnowledge Solution (ID 36.0.600194.2485190)) in the Check Point Technical Services site.

If the external IP address of the FireWall is an illegal address, can you connect to it via SecuRemote?

The SecuRemote client will be unable to connect to the FireWall.

When there is an external NAT device between the FireWall and the Internet, and the external IP address of the FireWall is not published, and the external NAT device is performing hide NAT, the packets issued by the SecuRemote client cannot be routed by the Internet to the destination.

Cause: If the external IP address of the FireWall is not published, there is no way for the SecuRemote client to find the FireWall.

See the SecureKnowledge Solution (ID 55.0.639947.2564039)) in the Check Point Technical Services site

“Leaky” NAT

For some connections, (usually those with long timeouts) the internal IP address of the Address Translated object “leaks” through VPN-1/FireWall-1. This sometimes causes the connection to fail since the reply is to an unknown IP address.

Cause

Leaky NAT is caused by the TCP timeout of that specific connection. When a TCP connection is inactive for too long, it is deleted from the NAT tables. If the connection is resumed, it will be inspected again on the inbound interface, but since it is an established connection and not a SYN packet it won’t be inspected on the Outbound interface, and will therefore be passed untranslated.

For a connection to be translated it needs to be in the NAT tables. If a connection is deleted from the NAT tables it will be deleted from the Connection tables as well. Occasionally, packets from connections that are no longer registered in the NAT tables or the connection tables pass through anyway. The reason could be that the connection is being checked and allowed through by the Rule Base even though it should not be.

Troubleshooting

The symptom for this behavior is usually a connection drop. This can be seen in the output of the `fw monitor` command, where the Internal IP address is seen on the outbound interface. That means that the server will be getting an unreachable IP address, causing the connection to fail.

How to workaround this issue

This issue can be overcome in a number of ways:

1. Increase the TCP timeout value

The TCP timeout parameter that is set in the GUI via the Properties > Security Policy Tab, or in the `objects.C file`. It decides the duration of an established but inactive (idle) connection. The default is set to 3600 Seconds.

In the GUI the value can be set to a maximum of 7200 sec. If a longer timeout is needed, it can be set to a higher value in the `Objects.C file`. If the policy is installed using the GUI the value in the GUI will overwrite the value in the `Objects.C` file. If the policy will be installed from a command line with the GUI closed, the value in the `Objects.C` file will be used.

2. Increase TCP timeout for a specific service

It is possible to set the timeout for a specific service. Make the following changes to the `init.def` file (`$FWDIR/lib`):

Add the line:
`ADD_TCP_TIMEOUT(<port>,<timeout>)`
before the line:
`ADD_TCP_TIMEOUT(0,0).`

`port` = TCP service port

`timeout` = Desired timeout.

3. Increase the value out of the TCP start time out (tcpstarttimeout) parameter

This workaround is for a situation where leaky NAT happens before the connection is established. When the initiator sends the initial SYN packet, the TCP Start Timeout parameter is set in the `objects.C` file, Its

default value is 1 Minute. This value is the waiting value between a SYN packet and a SYN-ACK packet. If this counter is timed out, the connection will be erased from the tables.

If the connection is resumed and is no longer in the tables it can pass with no translation because it is absent from the NAT tables.

In this scenario, one can increase the value of this parameter in order to increase the waiting period for the SYN-ACK packet. Bear in mind that this change will increase the size of the tables, because the deletion of each entry will be postponed.

4. Increase the value of the TCP end timeout (tcpendtimeout):

This workaround is for a situation where leaky NAT happens in the closing phase of the connection.

In the `Objects.C` file, set the `tcpendtimeout` value. The default value is 50 Seconds.

This is the waiting time between the time that the two peers sent their FIN or RESET packets, and the time that the last ACK was sent. When the time is exceeded, the connection is deleted from the tables. A packet that is sent through after that time will not be translated.

5. Change the relevant service to a service of type 'other' and not 'TCP':

This ensures that packets will be inspected on the outbound interface too.

6. Applying the ACK Denial-Of-Service hotfix.

The ACK DOS hotfix prevents packets in established TCP connections from being checked against the Rule Base. This way, if a connection is not registered in the tables, it will be dropped with no exceptions.

This workaround is rather extreme since it will drop each connection that has been idle for more than 3600 sec. It was originally developed to block Denial Of Service Attacks.

The following INSPECT code should be added to the `$FWDIR/lib/code.def` file (at the end of the file, just before the `#endif` statement).

After completing the edit, reinstall the security policy.

For version 4.0-based installations, this code will also log these events.

```
#ifndef ALLOW_NONFIRST_RULEBASE_MATCH
tcp, first or <conn> in old_connections or
(
#ifndef NO_NONFIRST_RULEBASE_MATCH_LOG
(
<ip_p,src,dst,sport,dport,0> in logged
) or (
record <ip_p,src,dst,sport,dport,0> in logged,
set sr10 12, set sr11 0, set sr12 0, set sr1 0,
log bad_conn
) or 1,
#endif
vanish
);
#endif
```

Debugging NAT

Note: See "Chapter 2: Troubleshooting Tools," page 5 for more information on the `fw ctl debug, fwinfo,` and the `fw monitor` commands.

To debug NAT problems, make use of the following debug commands. They should be issued in an environment that produces the problem.

For example, for an FTP connection problem, perform the commands followed by a FTP connection and some kind of "`snoop`" on the connection (`fw monitor` would be best)

This set of commands will produce some outputs that will shed some light over the issue.

Not all NAT problems require this kind of debugging. Use it for especially problematic situations, such as when NAT fails and for "Leaky" NAT issues.

Note: the commands should be issued in the order specified here.

1. From the `fw\bin` directory run:
   `fwtab –u > <file name>`

   This command prints the VPN-1/FireWall-1 connection and address translation tables. This allows you to check if the connections are in the tables.

   You should set the command to run every 30 seconds and to redirect the output to a file.

2. Run the following from the fw\bin directory:

   `fw ctl debug –buf`
   (Directs the information to a buffer)

   `fw ctl debug xlate xltrc`
   (This option is needed in FTP connection, in order to see the PORT command.)

   `fw ctl kdebug –f > <filename>`
   (Reads the information that was printed to the buffer by the previous command.)

   These commands will debug the translation procedure in the kernel and produce an output with the debug information.

NOTE: In order to stop the debugging issue `CTRL+C` after step 4 is completed

3. While these commands are running, run the fw monitor command that is appropriate for your connection. For a FTP connection for example run the following:

   ```
   fw monitor -m iIoO -e "accept [20:2,b]=21 or [22:2,b]=21 or [20:2,b]=20
   or [22:2,b]=20;" -o <filename>
   ```

4. Start the connection that will reproduce the problem.

   After the problem has occurred, stop the `fw monitor` command. Stop the debug command (as specified in step 2)

More Information

For more information on Network Address Translation, See

- Version 4.0: FireWall-1 Architecture and Administration User Guide Chapter 5
- Version 4.1: VPN-1/FireWall-1 Administration Guide Chapter 14
- Version 4.1 SP1 (Check Point 2000): VPN-1/FireWall-1 Administration Guide Chapter 14

Chapter 4: Troubleshooting Routers and Embedded Systems

In This Chapter

Introduction **30**

Management Server Architecture **30**

VPN-1/FireWall-1 configuration for a Nortel (Bay Networks) BayRS router **31**

Functions supported in VPN-1/FireWall-1 on Nortel routers 31
Common problems resolution 31
What happens when applying the Gateway rule to Interface and the direction set to “Eitherbound” 31
Problem which the time in log entries is different to the time on the router and the Management module. 31
Problem which the $FWDIR/log/fw.log file is growing out of proportion when using VPN-1/FireWall-1management module. 31
Problem which the remote Firewall is not dynamically downloading the correct policy 31
Problem, which the management module doesn’t get, logs from routers, few possible causes and resolution. 31
Problem which after installing policy, the system status will display HELP on a Nortel (Bay) Router 31
Does SynDefenser work on Nortel (Bay) router? 32
To configure a Nortel router with VPN-1/FireWall-1 32
Controlling the FireWall 32
Licenses 33
Problems and bugs 33
To configure an SNMP password on a Nortel (Bay) Router 33
Further security considerations 34
BayRS Router Commands 34
Router Log Command: 34
Router Status Commands 34
Router Kernel Information Commands 34
VPN-1/FireWall-1 Commands: 35
General Commands 35
Main Bay Command Console (BCC) Commands 35
How to configure VPN-1/FireWall-1 using BCC 35
Debugging Nortel (Bay) Routers 36
General problems 36
When the connection timed out while trying to install policy 37

VPN-1/FireWall-1 configuration for a Xylan switch **38**

Functions supported in VPN-1/FireWall-1 on Xylan Switch 38
Common problems resolution 38
Problem which the remote Firewall is not dynamically downloading the correct policy 38
Problem, which the management module doesn’t get, logs from routers, few possible causes and resolution. 38
Problem which you can’t load policy into xylan module and you receive an “unauthorized action” error message. 38

Debugging Routers and Embedded systems **39**

Information to Gather 39
BAY Router 39
Xylan 39

More Information **40**

Troubleshooting Routers and Embedded Systems

Introduction

A VPN-1/FireWall-1 enforcement point is a machine or device that enforces at least some part of the Security Policy. An enforcement point can be a workstation, router, switch or any machine that can be managed by a Management Module by installing a Security Policy or an Access List.

This chapter provides additional information about routers and embedded systems, not covered in the User Guides.

VPN-1/FireWall-1 can communicate with Nortel and Xylan routers. This section of this chapter dealing with Nortel concentrates on how to operate and debug Nortel routers, and the related VPN-1/FireWall-1 commands. The smaller section on Xylan routers offers some solutions to common problems.

Management Server Architecture

The Check Point Management Server Architecture can centrally manage multiple platforms and Embedded Systems simultaneously. The interaction of the Router/switch with the Management Server (or Control Module) is very important. The Security Policy is compiled on the management server, and downloaded to the Firewall Module located on the Router/switch.

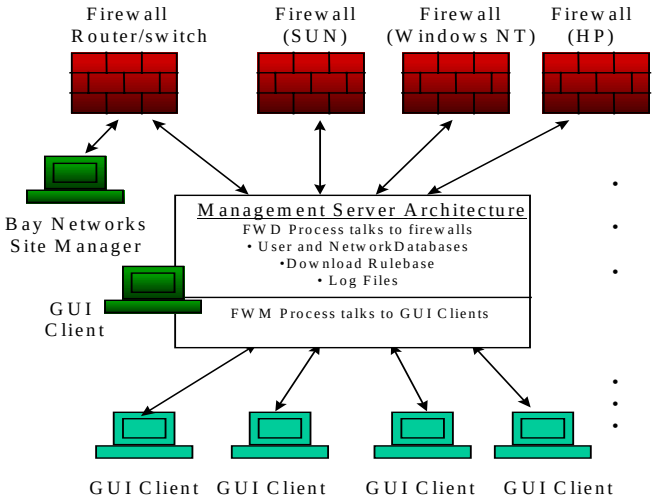


Figure 1. General architecture of the interaction between Management Server (Control Module) and the Firewall Module on the Embedded System

Management Server to Embedded Firewall Communications

- S/Key Authentication scheme between Management Server and Embedded System
- Router (Embedded System) sends log file information back to Management Server on port 257
- Management Server Downloads Rule Base to Embedded System on Port 256

Management Server to GUI Client Communications

- Communication between Management Server and GUI Client (including Username/Password) is encrypted on port #258

VPN-1/FireWall-1 configuration for a Nortel (Bay Networks) BayRS router

Functions supported in VPN-1/FireWall-1 on Nortel routers

The functions supported in VPN-1/FireWall-1 on a Nortel (Bay Networks) BayRS router are:

- Accept/Reject rules
- Logs and Alerts
- Anti-Spoofing
- Time objects (for version 4.1 and higher)

Common problems resolution

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

What happens when applying the Gateway rule to Interface and the direction set to “Eitherbound”

See the SecureKnowledge Solution (ID: 10022.0.1673175.2471537) in the Check Point Technical Services site

Problem which the time in log entries is different to the time on the router and the Management module.

See the SecureKnowledge Solution (ID: 3.0.666864.2300662) in the Check Point Technical Services site

Problem which the $FWDIR/log/fw.log file is growing out of proportion when using VPN-1/FireWall-1management module.

See the SecureKnowledge Solution (ID: 10043.0.4387594.2572347) in the Check Point Technical Services site

Problem which the remote Firewall is not dynamically downloading the correct policy

See the SecureKnowledge Solution (ID: 10022.0.1673144.2471537) in the Check Point Technical Services site

Problem, which the management module doesn’t get, logs from routers, few possible causes and resolution.

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Problem which after installing policy, the system status will display HELP on a Nortel (Bay) Router.

See the SecureKnowledge Solution (ID: 55.0.3594400.2592864) in the Check Point Technical Services site

Does SynDefenser work on Nortel (Bay) router?

See the SecureKnowledge Solution (ID: 36.0.764381.2490623) in the Check Point Technical Services site

To configure a Nortel router with VPN-1/FireWall-1

Do the following

1. Perform a regular installation of the router (`boot bn/asn/arn.exe ti.cfg`, and then `install.bat`), or use a predefined non-FireWalled configuration, if you have one. The important thing is that the router is configured so that communication from Nortel's Site Manager to the router is enabled.
2. Through the Configuration Manager (a GUI for controlling several routers), make sure that all the non-FireWalled details (like IP Circuits, protocols, etc.) are configured the way you would like them to be.
3. In Configuration Manager, perform the following steps:
   1) Select Platform FireWall Create and press the OK button in the displayed pop-up window.
   2) Select Platform FireWall Parameters, specify the host to which you would like to send Logs (VPN-1/FireWall-1 Management station) and the local host address (the router's main address). You may also configure a secondary and tertiary backup log servers that will be used in case of failure to communicate with the main one.
   3) Select Platform FireWall Interfaces and press the OK button in the displayed pop-up window.
   4) Select File Save As, and save the file as any name you like (`fw.cfg`, for instance).
5. On the router's console type the command:
   `fwputkey <password> <FireWall-1 Management IP>`.
   On the VPN-1/FireWall-1 Management station, type the command:
   `fw putkey -p <password> <router IP>`.
   Repeat these commands with the secondary and tertiary log servers IPs
6. On the router's console type the command:
   `boot asn.exe fw.cfg` - for ASN routers, or
   `boot arn.exe fw.cfg` - for ARN, or
   `boot bn.exe fw.cfg` - for BLN or "larger" routers.
7. Through the VPN-1/FireWall-1 GUI, define the router as a Network Object by selecting Router from the pull-down menu. In General tab select Bay Networks for the Type field, check the Internal checkbox, and the VPN-1/FireWall-1 Installed checkbox. Note that you cannot issue SNMP Fetch at this stage, since a default policy, which allows only FireWall communication between the management and the router, is installed on the router. You should also specify the external interface of the router, and the license mode (i.e., how many nodes can the router protect). Having defined the above, you should be able to install policies on the router, as if it were a regular inspection module (which it is).
8. Configuring Anti-spoofing is a little trickier. To do that perform, the following steps:
   1) Install a policy, which enables SNMP from the FireWall Management to the router, on the router.
   2) Create SNMP Fetch for the router.
   3) **Manually** change the fetched interface names (E121, E22, etc.) to `lin` **if the router image version is until 13.10 (including), or** `pol` **for versions 13.20 and above.**
   4) Define anti-spoofing as usual.

Controlling the FireWall

Bay routers only run VPN-1/FireWall-1 Inspection Module. You must have a Management Station to control it.

Licenses

The license for the embedded system capabilities is installed only on the Management Module – NOT on the router.

Problems and bugs

- **Sometimes there are no log entries**: Additional `putkey`s and `fwstop/fwstart` at the VPN-1/FireWall-1 Management, as well as boots to the router, usually fix this.
- **Anti-Spoofing:** As mentioned in “configuration Manager” under “To configure a Nortel router with VPN-1/FireWall-1”), interface names should be manually modified.
- **The router is not displayed on System Status:** Caused by not selecting Platform FireWall Interfaces. The Management displays that a policy had been installed, but it has no effect. In this case, the policy is accepted by the router, but there are no FireWalled interfaces on which to install the policy.

To configure an SNMP password on a Nortel (Bay) Router

To enable VPN-1/FireWall-1 to correctly communicate with the Nortel (Bay) router via SNMP, do the following during configuration:

On the Nortel Site Manager:

1. Select the router you would like to configure (there is a small window which lists all the routers the Site Manager "knows" about).
2. From the Site Manager Menu bar, choose Tools Configuration Manager Dynamic. This will open a Configuration Manager window, which lets you configure a specific router.
3. Save the current configuration file (File Save As `somename.cfg`), so you'll be able to return to this state at a later time, by simply booting the router with this configuration file.
4. On the configuration Manager choose Protocols IP SNMP Communities. This will open a window called "SNMP Community List".
5. On the SNMP Community List Window, choose Community Add Community, to add your own community, giving it READ/WRITE permissions.
6. Select the new community that you've defined in step 5, and choose Community Managers. This will open the Managers window. In this window, add the IP address of the VPN-1/FireWall-1 machine.
7. Exit the "Managers" and the SNMP Community List windows (Don't erase the "Public" default community yet. Do it later).
8. In the Configuration Manager, save your definition in a file, preferably with the ".cfg" suffix (File Save As).

To enable VPN-1/FireWall-1 to correctly communicate with the Nortel (Bay) router via SNMP, make sure that the following steps are performed during configuration:

In the VPN-1/FireWall-1 GUI

1. Open the Network Objects Manager, and define the router. The definitions should be as follows:

```
Type = Router
Location = Internal
Vendor = Bay Networks
FireWall-1 = Not Installed
```

2. Press the "SNMP Info..." button to Enter the "SNMP Information" window, and in it change the values of both "Read" and "Write" fields to the new community you've defined previously using the Nortel (Bay) Site Manager.
   Make rules which have either "Routers" or the specific router in the "Install On" field.

Warning - Make sure that you are not adding rules which block SNMP communication between VPN-1/FireWall-1 and the router, and from the Site Manager to the router.

3. Install the policy. This should load the access list on the router.

Further security considerations

After you've done all the above, note the following considerations:

1. Preventing illegal SNMP access to your router:
   - Using Configuration Manager, as described above, erase the default "Public" community, or make it READ ONLY.
   - Whatever access list you make, it is recommended you allow SNMP connections to the router only from the VPN-1/FireWall-1 site and from the Site Manager. No other SNMP connections to the router should be allowed (this, of course, doesn't include SNMP THROUGH the router, to different locations, which is simply a matter of your security policy choices).
2. It is recommended that you copy the configuration file on the router to a special file called "`config`" (no extensions), which is the default configuration file, used when the router comes up from a failure (when turned on, after a power supply failure, etc.). This, of course, should only be done after you verified everything is OK with your configuration file.

BayRS Router Commands

There are some important commands that can be run on the Technicians Interface (TI).

To log into the TI (the command line of the router) you can telnet, or use a console, to connect to the router and login in as user “Manager” without any password. The exception to this is the BayRS 5000 in which each slot functions as a separate router and is configured separately. In this case, when connecting to the BayRS 5000 you will be presented with a menu displaying all the boards currently installed. Select the one you wish to configure and then select the TI option.

The following are a list of typical commands that can be run on the command line of the router.

Router Log Command:

Display all log messages from the firewall code running on slot 3 for example:

```
log -fwitdf –eRFWALL –s3
```

Router Status Commands

To show the current state and ip address of all the circuits/interfaces:

```
show ip circuit
```

To show the currently established TCP connections (connections to the router itself):

```
show tcp connections
```

Router Kernel Information Commands

To show the amount of RAM on each slot:

```
get wfHwEntry.31.*
```

To show the amount of memory used on each slot:
```
get wfKernelEntry.2.*
```

To show the amount of memory free on each slot:
```
get wfKernelEntry.3.*
```

VPN-1/FireWall-1 Commands:

To save the "secret" password for use in connecting and communicating with the management station:
```
fwputkey secret xxx.xxx.xxx.xxx
```

To erase all the current password entries in the NVRAM.
```
fwputkey clearkey
```

To retrieve VPN-1/FireWall-1 configuration (MIB)
```
get wfRFwallGroup.*.0
```

General Commands

To show the version and build date of the current boot image.
```
stamp
```

To start BCC (Bay Command Console) the configuration utility.
```
bcc
```

Main Bay Command Console (BCC) Commands

There are also a few commands that may be run from the Bay Command Console (BCC), the utility used to configure the router (create configuration files). Entering BCC can be accomplished by typing bcc at the command line. The following are a list of commands that can be run on the command line of the router.

To enter the configuration:
```
config
```

To shows total memory usage on the router:
```
show proc mem total
```

To shows a breakdown of memory usage by the various modules:
```
show proc mem detail
```

BCC Configuration Commands:

To display all the current configuration information:
```
display
```

To list Objects and display a listing of all the currently defined objects and services at the current configuration tree level.
```
lso
```

This displays configuration information for the current level. Typing the variable name followed by the new value can modify these values.

How to configure VPN-1/FireWall-1 using BCC

The following is an example of how to configure the firewall in BCC.

1. First enter the IP directory by typing:

   ip

2. Next type the following command to configure the primary management station IP address and the local IP address (the routers primary interface):

```
firewall pri 1.1.1.1 loc 2.2.2.2
```

3. Typing `info` at this point will show you the currently defined firewall information. Back up management stations can be defined at this point.
4. Now the individual interfaces must be configured to use the firewall. Type **`back`** twice to return to the root menu. Type in the name of the first interface:

   ```
   ethernet/1/1
   ```

5. Now type in the ip address string:

   ```
   ip/1.1.1.1/255.255.255.0
   ```

6. Now type the key word*:*

   ```
   firewall
   ```

   Now the firewall is configured to run on this interface. Typing *info* at this point will display information concerning the firewall on this interface. It is here that you will find the policy-index number, which for firewall purposes is the interface name (pol1 etc.). These policy-index numbers are automatically assigned a unique number each time an interface is configured. It is possible to change some or all of these policy-indexes to be the same, in which case the firewall will treat them all as the same interface.
7. Repeat the configuration for all interfaces running the firewall.

Debugging Nortel (Bay) Routers

General problems

To debug general problems, you can start with the following steps:

1. Log into the Technician Interface (TI).
2. Check the log files on the router. RFWALL is a keyword in the log files for the Check Point Software on the Router. The proper syntax for this is

   `Log -ffdwit -eRFWALL` (will show all of the new firewall messages.)

   `(-ffdwit)` means
   `(ff)` fault
   `(d)` debug
   `(w)` warning
   `(i)` informational
   `(t)` trace
   `log -ffdwit -t9:00` (will show messages after 9:00)
3. The MIB Group for the firewall is wfRFwallGroup. The following MIB objects will show the IP Addresses of the Check Point Control Station, and the Firewall Module on the Router.

   ```
   get wfRFwallGroup.*.0
   ```

   The output of the command retrieves the following data, which present the current router's VPN-1/FireWall-1 configuration:

   ```
   wfRFwallGroup.wfRFwallDelete.0 = 1
   wfRFwallGroup.wfRFwallDisable.0 = 1
   wfRFwallGroup.wfRFwallState.0 = 1
   wfRFwallGroup.wfRFwallLogHostIp.0 = xxx.xxx.xxx.xxx
   wfRFwallGroup.wfRFwallLogHostIpInt.0 = 0
   wfRFwallGroup.wfRFwallLocalHostIp.0 = yyy.yyy.yyy.yyy
   ```

```
wfRFwallGroup.wfRFwallLocalHostIpInt.0 = 0
wfRFwallGroup.wfRFwallVersion.0 = 2
wfRFwallGroup.wfRFwallHmemMin.0 = 50000
wfRFwallGroup.wfRFwallHmemMax.0 = 100000
wfRFwallGroup.wfRFwallLogHostIpBkp1.0 = 0.0.0.0
wfRFwallGroup.wfRFwallLogHostIpIntBkp1.0 = 0
wfRFwallGroup.wfRFwallLogHostIpBkp2.0 = 0.0.0.0
wfRFwallGroup.wfRFwallLogHostIpIntBkp2.0 = 0
```

When the connection timed out while trying to install policy

1. Check the communications from the management station to the router. Make sure you can ping the router from a DOS Prompt using the IP address.
2. Next, check to see if you can ping the router using the name described for the object in the Network Object Manager. On Windows NT, the “hosts” file is located under \winnt\system32\drivers\etc\hosts. Check to see if the name in this file can be resolved.
3. If you still have problems downloading a Rule Base, try and synchronize the secret keys between the Check Point Management Station and the Nortel (Bay) Router as follows:

   On the router, type in
   `fwputkey` `<secret key> <IP Address of Check Point Management Station>`

   On the management station
   `fw putkey` `<secret key> <IP Address of Router>`
4. The `fw bload` command could be used to compile and install the security policy on the embedded module. You can use this command from the command line.

   Command’s syntax:
   `fw bload` `[inspect-file | rule-base] target…`

VPN-1/FireWall-1 configuration for a Xylan switch

You should have a management control module. It is called the Enterprise Management Console or EMC (VPN/FireWall management module). For a switch to support VPN-1/FireWall-1 functionality it requires a licensed inspection module (VPN/FireWall module). Due to other resident networking and switching software, 16MB DRAM is a minimum requirement but 32 or 64 MB is recommended.

After preparing the Xylan Switch hardware you should simply configure the Xylan switch Network object through the VPN-1/FireWall-1 GUI and establish authentication between the VPN-1/FireWall-1 management (using the command "`fw putkey`" on the management) and the Xylan switch (using the command "`fwconfig`" on the Switch). To configure the VPN/FireWall inspection module and to display its current configuration on the Xylan switch use the "`fwconfig`" command.

Functions supported in VPN-1/FireWall-1 on Xylan Switch

The functions supported in VPN-1/FireWall-1 on a Xylan switch are:

- Accept/Reject rules
- Logs and Alerts
- Anti-Spoofing
- Time objects (version 4.1 and higher)

Common problems resolution

Problem which the remote Firewall is not dynamically downloading the correct policy

10022.0.1673144.2471537

See the SecureKnowledge Solution (ID: 10022.0.1673144.2471537) in the Check Point Technical Services site

Problem, which the management module doesn't get, logs from routers, few possible causes and resolution.

10022.0.527050.2411096

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Problem which you can't load policy into xylan module and you receive an "unauthorized action" error message.

55.0.634804.2563934

See the SecureKnowledge Solution (ID: 55.0.634804.2563934) in the Check Point Technical Services site

Debugging Routers and Embedded

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

This section lists the information that Check Point Support will ask you to gather for problem related to Troubleshooting Routers and Embedded Systems. It may also be of use when doing your own troubleshooting.

See **Error! Cannot open file.** for more information on the `fwinfo, fw monitor` and the `fw ctl debug` commands.

Information to Gather

BAY Router

1. Router's `config` file.
2. Output of `stamp` command.
3. Router model (BLN, ASN, ARN).
4. `Control.map` and `clients` files.
5. `fwinfo` of the management.

Send the files to support@ts.checkpoint.com.

Bay CES

1. CES image version.
2. `fwinfo` of the management.
3. `fwinfo` of the module (CES).

Send the files to support@ts.checkpoint.com.

Xylan

1. Image version (if it's newer than 3.1.6 then, send the image files).
2. `Control.map` and `clients` files.
3. `fwinfo` of the management.

Send the files to support@ts.checkpoint.com.

More Information

For more information on Routers and Embedded Systems, See

Version 4.1 SP1

Check Point 2000 Administration Guide:
Chapter 17 Routers and Embedded Systems.
Chapter 4: Network objects, Router properties, pages 118-141

Version 4.1

Administration Guide:
Chapter 17 Routers and Embedded Systems.
Chapter 4: Network objects, Router properties, pages 114-139

Version 4.0

FireWall-1 Architecture and Administration User Guide version 4.0:
Chapter 6: Routers and Embedded Systems.

Managing FireWall-1 Using the Windows GUI, pages 35-48

Chapter 5: Troubleshooting Open Security Extension

In This Chapter:

Introduction 42

Nortel (Bay) Routers: Configuration and Problem Resolution 42

To configure an SNMP password on a Nortel (Bay) Router 42
Further security considerations 43
Common problems resolution for Nortel Routers 43
Cannot get logs from the router 43
Error message while trying to install new license (only for 4.1) 43
What methods of packet filtering can a Bay router handle? 43
OSE does not work when Anti Spoofing is set to other+ 44

Cisco Routers: Problem Resolution and Debugging 44

Differences between Cisco router version 9 and 11: Support for Anti-Spoofing 44
Common problems resolution for Cisco Routers 44
Multiple logs received from the Cisco router 44
Error message on the Import Access List window of the FireWall-1 GUI 44
Cannot get logs from the router 44
Error message while trying to install new license (only for 4.1) 44
OSE does not work when Anti Spoofing is set to other+ 44
Access List download fails the first time a username is defined in the router's enable mode 44
Debugging of Cisco Routers 44

Cisco Pix Firewall: Problem Resolution 45

Common problems resolution for Cisco PIX Firewall 45
Warning message when installing policy on Cisco PIX 45
Cannot get logs from the router 45
Error message while trying to install new license (only for 4.1) 45
OSE does not work when Anti Spoofing is set to other+ 45
Tips for successfully installing a policy on a PIX device 45

3COM routers: Problem Resolution and Debugging 46

Common problems resolution for 3Com Routers 46
Cannot get logs from the router 46
Error message while trying to install new license (only for 4.1) 46
OSE does not work when Anti Spoofing is set to other+ 46
Debugging of 3Com Routers 46

Microsoft RRAS (SteelHead) Routers: Problem Resolution and Debugging 47

Common problems resolution 47
Cannot get logs from the router 47
Error message while trying to install new license (only for 4.1) 47
OSE does not work when Anti Spoofing is set to other+ 47
Debugging for Microsoft RRAS (SteelHead) 47

More Information 47

Troubleshooting Open Security Extension

Introduction

Open Security Extension is a product that enables a VPN/FireWall management module to generate and download Access Lists and configure security for routers (3com, Nortel, Microsoft RRAS (Steelhead), and Cisco) and Integrated FireWall (Cisco PIX).

This chapter provides additional information about Routers, not covered in the User Guides.

A VPN/FireWall management module can manage Access Lists for the following third-party routers and devices. Any number of routers and devices can be managed:

- Bay Networks Routers: version 7.x - 12.x
- Cisco Routers: IOS version 9,10,11,12 — Note that version 12 is only for VPN-1/FireWall-1 4.1
- Cisco PIX Firewall: version 3.0, 4.0, 4.1x — Note that Open Security Extension supports only two PIX interfaces: the internal and external interfaces.
- 3Com Netbuilder: version 9.x
- Microsoft Routing and Remote Access Service RRAS (SteelHead) for Windows NT Server 4.0

Nortel (Bay) Routers: Configuration and Problem Resolution

When creating access list for Nortel router, be aware that Nortel router access lists always include an implicit final rule that accepts all communications (any, any, accept). You must explicitly define a final rule in the Rule Base that drops all communications not described by the other rules (Any / Any / Drop)

To configure an SNMP password on a Nortel (Bay) Router

To enable VPN-1/FireWall-1 to correctly communicate with the Bay router via SNMP, do the following during configuration:

On the Nortel Site Manager:

1. Select the router you would like to configure (there is a small window which lists all the routers the Site Manager "knows" about).
2. From the Site Manager Menu bar, choose Tools Configuration Manager Dynamic. This will open a Configuration Manager window, which lets you configure a specific router.
3. Save the current configuration file (File Save As `somename.cfg`), so you'll be able to return to this state at a later time, by simply booting the router with this configuration file.
4. On the configuration Manager choose Protocols IP SNMP Communities. This will open a window called "SNMP Community List".
5. On the SNMP Community List Window, choose Community Add Community, to add your own community, giving it READ/WRITE permissions.
6. Select the new community that you've defined in step 5, and choose Community Managers. This will open the Managers window. In this window, add the IP address of the VPN-1/FireWall-1 machine.

7. Exit the "Managers" and the SNMP Community List windows (Don't erase the "Public" default community yet. Do it later).
8. In the Configuration Manager, save your definition in a file, preferably with the ".cfg" suffix (File Save As).

To enable VPN-1/FireWall-1 to correctly communicate with the Bay router via SNMP, make sure that the following steps are performed during configuration:

In the VPN-1/FireWall-1 GUI

1. Open the Network Objects Manager, and define the router. The definitions should be as follows:

```
Type = Router
Location = Internal
Vendor = Bay Networks
FireWall-1 = Not Installed
```

2. Press the "SNMP Info..." button to Enter the "SNMP Information" window, and in it change the values of both "Read" and "Write" fields to the new community you've defined previously using Bay's Site Manager. Make rules which have either "Routers" or the specific router in the "Install On" field.

Warning - Make sure that you are not adding rules which block SNMP communication between FireWall-1 and the router, and from the Site Manager to the router.

3. Install the policy. This should load the access list on the router.

Further security considerations

After you've done all the above, take note of the following considerations:

1. Preventing illegal SNMP access to your router:
   - Using Configuration Manager, as described above, erase the default "Public" community, or make it READ ONLY.
   - Whatever access list you make, it is recommended you allow SNMP connections to the router only from the VPN-1/FireWall-1 site and from the Site Manager. No other SNMP connections to the router should be allowed (this, of course, doesn't include SNMP THROUGH the router, to different locations, which is simply a matter of your security policy choices).
2. It is recommended that you copy the configuration file on the router to a special file called "`config`" (no extensions), which is the default configuration file, used when the router comes up from a failure (when turned on, after a power supply failure, etc.). This, of course, should only be done after you verified everything is OK with your configuration file.

Common problems resolution for Nortel Routers

Cannot get logs from the router

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Error message while trying to install new license (only for 4.1)

See the SecureKnowledge Solution (ID: 10043.0.4395816.2572453) in the Check Point Technical Services site

What methods of packet filtering can a Bay router handle?

See the SecureKnowledge Solution (ID: 47.0.4030890.2554461) in the Check Point Technical Services site

OSE does not work when Anti Spoofing is set to other+

See the SecureKnowledge Solution (ID: 10043.0.6958228.2640175) in the Check Point Technical Services site

Cisco Routers: Problem Resolution and Debugging

Differences between Cisco router version 9 and 11: Support for Anti-Spoofing

Version 9 routers do not support anti-spoofing. These routers do not distinguish between inbound and outbound or outbound. All you can do is install a Security Policy on a router interface.

Versions 10 and 11 support anti-spoofing because it is possible to define inbound or outbound filter directions.

Common problems resolution for Cisco Routers

Multiple logs received from the Cisco router

See the SecureKnowledge Solution (ID: 10022.0.1673181.2471537) in the Check Point Technical Services site

Error message on the Import Access List window of the FireWall-1 GUI

Importing access list operation will fail when trying to import in Graphical rulebase from a FastEthernet0/0 interface

See the SecureKnowledge Solution (ID: 10043.0.5516028.2585580) in the Check Point Technical Services site

Cannot get logs from the router

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Error message while trying to install new license (only for 4.1)

See the SecureKnowledge Solution (ID: 10043.0.4395816.2572453) in the Check Point Technical Services site

OSE does not work when Anti Spoofing is set to other+

See the SecureKnowledge Solution (ID: 10043.0.6958228.2640175) in the Check Point Technical Services site

Access List download fails the first time a username is defined in the router's enable mode

When a username is defined in the router's enable mode, downloading the Access List fails. Every time the router asks for a username, a time-out message is displayed. Access List installation will succeed on the second try. To avoid this problem, do not define enable username for Cisco routers.

Debugging of Cisco Routers

To verify whether the VPN-1/FireWall-1 installed the access list correctly on the router, use the following router command to display the current configuration in detail, including the access lists.

```
Show running-config
```

When having trouble installing the access list from the VPN-1/FireWall-1 GUI you could use the following command from command line (on the VPN/FireWall management module):

```
router_load –cisco
```

Syntax

```
router_load -cisco <router> <conf file> <password|XXX|PROMPT> <enable
password|XXX|PROMPT>
```

OR:

```
router_load -cisco <router> <conf file> <user name|XXX|PROMPT>
<password|XXX|PROMPT> <enable user name|XXX|PROMPT> <password|XXX|PROMPT>
```

OR:

```
router_load -cisco <router> <password|XXX|PROMPT> <enable
password|XXX|PROMPT> [-command <command>]
```

OR:

```
router_load -cisco <router> <user name|XXX|PROMPT> <password|XXX|PROMPT>
<enable user name|XXX|PROMPT> <password|XXX|PROMPT> [-command <command>]
```

The `conf` file is the `router.cl` file in the `conf` directory. This file doesn't exist when configuring the router network object on the VPN-1/FireWall-1 GUI. You can create this file by installing the access list from the GUI (when the router is not connected to the VPN/FireWall management module).

Cisco Pix Firewall: Problem Resolution

The PIX Firewall contains two Ethernet interfaces, one for the inner, secure network, and the other for the outer, unprotected network.

The inside network is invisible from the outer network.

Before address translation rules are supplied, communication between outside and inside is blocked.

Common problems resolution for Cisco PIX Firewall

Warning message when installing policy on Cisco PIX

The cause is that Address Translation has not been configured

See the SecureKnowledge Solution (ID: 10043.0.5956180.2591133) in the Check Point Technical Services site

Cannot get logs from the router

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Error message while trying to install new license (only for 4.1)

See the SecureKnowledge Solution (ID: 10043.0.4395816.2572453) in the Check Point Technical Services site

OSE does not work when Anti Spoofing is set to other+

See the SecureKnowledge Solution (ID: 10043.0.6958228.2640175) in the Check Point Technical Services site

Tips for successfully installing a policy on a PIX device

See the SecureKnowledge Solution (ID: 55.0.4011754.2602886) in the Check Point Technical Services site

3COM routers: Problem Resolution and Debugging

Common problems resolution for 3Com Routers

Cannot get logs from the router

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Error message while trying to install new license (only for 4.1)

See the SecureKnowledge Solution (ID: 10043.0.4395816.2572453) in the Check Point Technical Services site

OSE does not work when Anti Spoofing is set to other+

See the SecureKnowledge Solution (ID: 10043.0.6958228.2640175) in the Check Point Technical Services site

Debugging of 3Com Routers

To verify whether the VPN-1/FireWall-1 installed the Access List correctly on the router you can use router commands:

First, run the following command in order to list the current filters:

```
Show –fw filters
```

Second, run the following command using the name of the relevant access list (which you retrieve when using the first command) in order to show the content of the filter.

When having trouble installing the access list from the VPN-1/FireWall-1 GUI you could use the following command from command line (on the VPN/FireWall management module):

```
router_load -3com
```

Syntax

```
router_load -3com <router> <conf file> <user name|XXX|PROMPT>
<password|XXX|PROMPT> <enable password|XXX|PROMPT> [-command <command>]
```

The `conf` file is the `router.cl` file in the `conf` directory. This file doesn't exist when configuring the router network object on the VPN-1/FireWall-1 GUI. You can create this file by installing the Access list from the GUI (when the router is not connected to the VPN/FireWall management module).

Microsoft RRAS (SteelHead) Routers: Problem Resolution and Debugging

Common problems resolution

Cannot get logs from the router

See the SecureKnowledge Solution (ID: 10022.0.527050.2411096) in the Check Point Technical Services site

Error message while trying to install new license (only for 4.1)

See the SecureKnowledge Solution (ID: 10043.0.4395816.2572453) in the Check Point Technical Services site

OSE does not work when Anti Spoofing is set to other+

See the SecureKnowledge Solution (ID: 10043.0.6958228.2640175) in the Check Point Technical Services site

Debugging for Microsoft RRAS (SteelHead)

When having trouble installing the access list from the VPN-1/FireWall-1 GUI you could use the following command from the command line (on the VPN/FireWall management module):

```
router_load -steelhead
```

Syntax:

```
router_load -steelhead <router> <conf file> <user name|XXX|PROMPT>
<password|XXX|PROMPT> [-command <command>]
```

The `conf` file is the `router.cl` file in the `conf` directory. This file doesn't exist when configuring the router network object on the VPN-1/FireWall-1 GUI. You can create this file by installing the Access list from the GUI (when the router is not connected to the VPN/FireWall management module).

More Information

For more information on Managing Router Access Lists, see:

Version 4.1 SP1

Check Point 2000 Administration Guide
Chapter 4: Network objects, Router properties, pages 118-147,
Chapter 14: Network Address Translation, pages 464-470.

Version 4.1

Administration Guide
Chapter 4: Network objects, Router properties, pages 115-145,
Chapter 14: Network Address Translation, pages 459-464.

Version 4.0

Managing FireWall-1 Using the Windows/OpenLook GUI User Guide,
Chapter 2: Network Objects, Router Setup, page 40.

Chapter 6: Troubleshooting Anti-Spoofing

In This Chapter:

Introduction **49**

Common Problems Resolution **49**

Meaning of log message: Rule 0 – spoof attempt 49
Using virtual interfaces with anti-spoofing 49
BOOTP and Anti- Spoofing 49
How to configure anti-spoofing with DHCP protocol 50
How to prevent broadcast messages from being rejected as spoofing attacks 50
Static ARP and Anti-Spoofing 50

Debugging Anti-Spoofing **51**

Information to Gather 51

Troubleshooting Anti-Spoofing

Introduction

Spoofing is a technique where an intruder attempts to gain unauthorized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges. VPN-1/FireWall-1 has a sophisticated anti-spoofing feature, which detects such packets by requiring that the interface on which a packet enters a gateway corresponds to its IP address.

Common Problems Resolution

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

Meaning of log message: Rule 0 – spoof attempt

Rule Zero is the rule VPN-1/FireWall-1 adds before the rules in the Rule Base to implement Anti-spoofing, dropping of packets with IP options, and some aspects of Authentication. Anti-spoofing is implemented before any rules are applied, so anti-spoof track logging shows rule zero as the relevant rule.

Using virtual interfaces with anti-spoofing

VPN-1/Firewall-1 ignores the virtual interfaces feature of Solaris, so that filtering and anti-spoofing is done on the physical interface.

If you want to use virtual interfaces with Anti-Spoofing, you need to define two network objects, one for each subnet, and then create a network group that combines them. Then you can put the group in the physical interface's Anti-Spoofing entry, just as you would if there was another physical network connected to the interface's network via a gateway.

See the SecureKnowledge Solution (ID: 3.0.698687.2304823) in the Check Point Technical Services site

BOOTP and Anti- Spoofing

The `bootp` protocol consists of two simple UDP protocols: bootpc (from the client, which boots to the server where the boot image is held) on port 67, and bootps (the other way around) on port 68. It is easy to define those two as UDP services in the GUI. The services normally use the broadcast address (255.255.255.255) as the client's address. Additional information is available in RFCs 951 and 1340.

In order to allow BOOTP, there are several things you should take care of:

1. Find out which address bootp clients use (normally it would be 255.255.255.255) and create a workstation network object with this IP.
2. Use this object as the source for the port 67 service and destination for the port 68 service.
3. Since bootp uses the IP broadcast address 255.255.255.255, you need to add it to the anti-spoofing group for the interface of the server, so that IP packets destined to it will be passed. Since the IP source address is often 0.0.0.0, you might also need that address to be part of the anti-spoofing group for the interface of the client (the device which attempts to boot). To do these things, you need to create a network object that will contain this address, so you'll be able to add it to the anti-spoofing group.

See the SecureKnowledge Solution (ID: 36.0.259529.2476199) in the Check Point Technical Services site

How to configure anti-spoofing with DHCP protocol

DHCP requests are being dropped on rule 0 in the log.

This is because FireWall-1 triggers the Anti-Spoofing, since it detects illegal addresses being broadcast when DHCP requests from the workstations try to get an IP address. This is seen by the FireWall as a spoof attempt.

To solve this,

1. Set up three Network Objects:
   - One group/network with the IP addresses of the network
   - A second object of type 'workstation' with an address of 0.0.0.0
   - A third object of type 'workstation' with an address of 255.255.255.255
2. Put them all in an Anti-Spoofing group
3. Apply that group to your interface for Anti-spoofing and install the new policy

See the SecureKnowledge Solution (ID: 3.0.216192.2211274) in the Check Point Technical Services site.

How to prevent broadcast messages from being rejected as spoofing attacks

There are two types of broadcast packets: those with a destination IP of 255.255.255.255 (which are broadcast all over the network) and those with a destination IP that is the IP of the network, with 1s in all the IP bits.

To include the first type, create a network object of type computer with the IP address 255.255.255.255. Then, create a group which will include both the localnet and the computer (broadcast-ip might not be a bad name for it) and put that group instead of the localnet as the allowed IP of the interface. You would also want the external interface to be not "others" but "others + broadcast-ip" because broadcasts can come from either direction.

To include the second type, check the "allow broadcasts" checkbox in the network's Network Object's Properties window.

See the SecureKnowledge Solution (ID: 36.0.2008729.2505025) in the Check Point Technical Services site.

Static ARP and Anti-Spoofing

ARP (address resolution protocol) is not an IP protocol. It is not forwarded to the TCP/IP protocol stack, so VPN-1/FireWall-1 does not filter it. However, it cannot be used to compromise the security of the internal network, because even if it causes a routing problem, anti-spoofing would still detect it.

Debugging Anti-Spoofing

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

This section lists the information that Check Point Support will ask you to gather for Anti-spoofing problems. It may also be of use when doing your own troubleshooting.

See “Chapter 2: Troubleshooting Tools,” page 5 for more information on the `fwinfo, fw monitor` and the fw ctl `debug` commands.

Information to Gather

1. `fwinfo` file
2. Network Diagram

Send the file to support@checkpoint.com

Chapter 7: Troubleshooting Security Servers and Content Security

In This Chapter:

HTTP Security server

How to Improve HTTP Security Server performance in a High Performance Environment....54

Environment 54
Hardware 54
IP Interface 55
The Software 55
VPN-1/FireWall-1 Rule Base 55
Diagram of the environment 56
Tuning....56
Performance Test 57
Conclusions 59

Resolving Common HTTP Security Server Problems....59

VPN-1/FireWall-1 Security server and HTTP 1.1....59
Client Authentication issues related to the HTTP Security Server....60
HTTP Security Server and DNS....61
How to use CVP for content security with HTTP and/or a URI service on ports other than 80 62
What rules are needed when setting up Content Security....62

Troubleshooting Security Server Performance problems....63

Test Plan....63

FTP Security Server

The FTP security server 66

Resolving Common FTP security server problems 66

FTP data connections are dropped by the FireWall....66
Allowing FTP data connections through the FireWall on random ports 68
Port command must end with a new line....68
Bi-directional FTP Data connection are not allowed 68
Fast mode and FTP....68
FTP connections hang during large file transfers....68
FTP PASV vulnerability: 69
PORT command is blocked....69
FTP commands being blocked by the FTP Security Server 69
PWD command is not enabled on the FTP server....69
How to cross several VPN-1/FireWall-1 Authentication Daemons....70
How to add a support for a new command to the ftp security server....70

SMTP Security Server

SMTP Email Process....71

The SMTP Security Server Process....72

Troubleshooting Common SMTP Security Server problems....73

Connection between the Email Client and the Firewall SMTP Security Server fails....73
Connection between the Firewall Mail Dequeuer and the Anti Virus Server fails....74
Connection between the Firewall Mail Dequeuer and the Final Email Server fails....74

Understanding the error handling mechanism of the SMTP daemon....74

How SMTP Security Server deals with envelope format....75

Log Viewer Error Messages....75

I. Error: "450 Mailbox Unavailable"....75
II. Error: "554 Mailbox unavailable" when trying to deliver mail....75
III. Error: "agent mail server ... reason: Too much mail data" in the Log Viewer....76
IV. Error: “Connection to Final MTA failed”....76

What commands are supported by the VPN-1/FireWall-1 SMTP Security Server?....77

More Information: Security servers and content Security....79

Debugging Security servers

Information to Gather....78

HTTP Security server

In This Section

This section describes how to Improve VPN-1/FireWall-1 HTTP Security Server performance in a High Performance Environment, and how to resolve and troubleshoot problems related to HTTP Security Servers

"How to Improve HTTP Security Server performance in a High Performance Environment", page 54

"Resolving Common HTTP Security Server Problems ," page 59

"How to Improve HTTP Security Server performance in a High Performance EnvironmentTroubleshooting Security Server Performance problems", page 63

See Also:
VPN-1/FireWall-1 Performance Tuning Guide

http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html

Suggests methods and techniques for improving various aspects VPN-1/FireWall-1 performance. The document is organized according to the VPN-1/FireWall-1 OS platform and the nature of the change (OS vs. VPN-1/FireWall-1 parameter tuning)

How to Improve HTTP Security Server performance in a High Performance Environment

One of the most effective ways of improving the performance of VPN-1/FireWall-1 is to increase the performance of the HTTP Security Server (`httpss`).

Using the `httpss` in a T-1 or less environment is fairly straight forward, whether doing content security, user authentication, URL logging or a combination of all of the above.

However, in environments where there is significant bandwidth to the Internet (i.e. greater than T-1), and where the number of concurrent users is large, (i.e. in the thousands) then the usage of `httpss` requires more planning, and tuning in order to perform at acceptable levels.

The following outlines a real life case (names excluded) in which the `httpss` is specifically performance tested with respect to the use of UFP and URL logging. The example includes hardware, software, tuning parameters, and observations. Hopefully it will provide some guidelines to implementing the HTTP security Server (`httpss`) in similar environments.

Environment

- Internet connection: 10 Mbps Ethernet
- Number of end users: 12,000

Hardware

Sun (TM) Enterprise 250 (2 X UltraSPARC-II 296MHz), Keyboard Present

OpenBoot 3.7, 512 MB memory installed,

AVAILABLE DISK SELECTIONS:

```
0. c0t0d0 <SUN4.2G cyl 3880 alt 2 hd 16 sec 135>
   /pci@1f,4000/scsi@3/sd@0,0
```

```
    1. c0t8d0 <SUN4.2G cyl 3880 alt 2 hd 16 sec 135>
       /pci@1f,4000/scsi@3/sd@8,0
```

AVAILABLE SWAP:

Total: 7848k bytes allocated + 1640k reserved = 9488k used, 400496k available

IP Interface

Issuing the **`ifconfig -a`** command resulted in:

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
      inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.1 netmask ffffff00 broadcast 192.168.1.255
      ether 8:0:20:a6:eb:58
hme1: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
      inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2..255
      ether 8:0:20:a6:eb:58
hme2: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
      inet 10.1.1.1 netmask ffffff00 broadcast 10.1.1.255
      ether 8:0:20:a6:eb:58
```

Issuing the **`/opt/CPfw1-41/bin/fw ctl iflist`** command resulted in:

```
0 : lo0
1 : hme0
2 : hme1
3 : hme2
```

The Software

- Solaris v2.6 SunOS 5.6 Generic_105181-16, (hardened according to customer's specifications)
- `Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 Build 41439 [VPN + DES + STRONG]`

VPN-1/FireWall-1 Rule Base

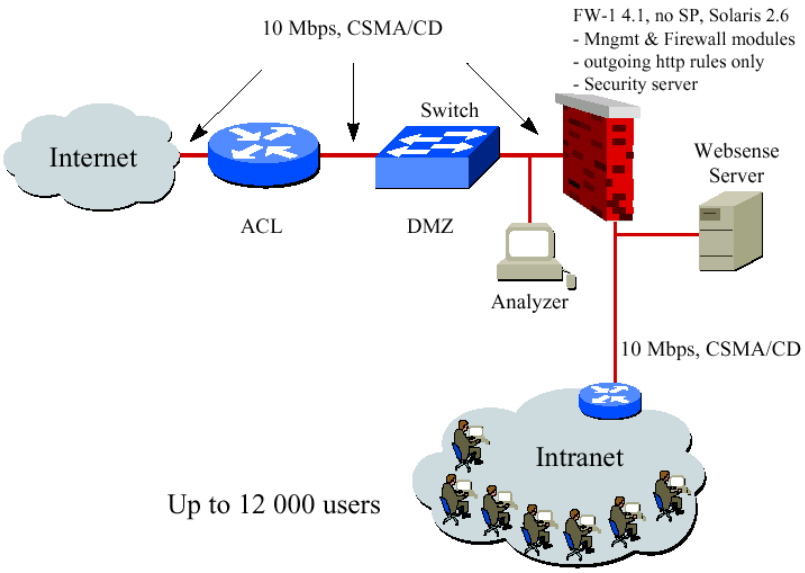
The rule base implemented is very simple, consisting of 4 rules.

Rule 1.	Stealth drop rule with track long.
Rule 2.	WebSense reject rule with track long.
Rule 3.	HTTP resource Accept rule for URL logging with track long.
Rule 4.	Clean-up drop rule with track long.

The number of objects defined was less than 200.

There is 1 NAT rule to hide internal subnets behind the VPN-1/FireWall-1 external IP address, although this rule is not really applicable since the transparent httpss proxy takes care of the connections without relying on NAT.

Diagram of the environment



Note: The WebSense Server was moved to a separate interface on the FireWall (100 Mbps Ethernet)

Tuning

System parameters

The following system parameters were set:

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
set rlim_fd_cur=4096
set rlim_fd_max=4096
set tcp:tcp_conn_hash_size = 16384
set fw:fwhmem = 0x1000000
```

TCP/IP stack parameters

The following TCP/IP stack parameters were set:

```
ndd -set /dev/hme adv_100fdx_cap 1
ndd -set /dev/tcp tcp_xmit_hiwat 65535
ndd -set /dev/tcp tcp_recv_hiwat 65535
ndd -set /dev/tcp tcp_cwnd_max 65535
ndd -set /dev/tcp tcp_slow_start_initial 2
ndd -set /dev/tcp tcp_conn_req_max_q 1024
ndd -set /dev/tcp tcp_conn_req_max_q0 4096
ndd -set /dev/tcp tcp_close_wait_interval 60000
```

VPN-1/FireWall-1 parameters

1. Increase connections table limit to 50,000, and hashsize to 65536.

   In `$FWDIR/lib/table.def` add to the end of line,
   `connections = limit 50000 hashsize 65536`

2. Increase `proxied_conns` table limit to 50,000

   In `$FWDIR/lib/table.def` add to the end of line
   `proxied_conns = limit 50000`

3. Increase NAT table limit to 50,000 and hashsize to 65536.

   In `$FWDIR/conf/objects.C` change the following lines,
   `:nat_limit (50000)`
   `:nat_hashsize (65536)`

4. Add `http_buffer_size` parameter (applies to VPN-1/FireWall-1 4.1):

   In `$FWDIR/conf/objects.C` add the line under props:
   `:http_buffer_size (32768)`

5. Increase the number of instances of the `in.ahttpd` HTTP security server process to 5

   In `$FWDIR/conf/fwauthd.conf` change the following line,
   `80 in.ahttpd wait -5`

Note: When using multiple instances of the security server— such as the `in.ahttpd` HTTP security server— the `client_was_auth` table is used. The `client_was_auth` table stores the port number of the specific security server to which the client connection was folded, so that subsequent connections from the same client will be handled by the same security server instance.

Performance Test

A test was conducted during a peak load period, which coincided with lunchtime during a Wednesday, with poor weather. (A likely scenario for maximum number of users sitting at their desktops, having lunch and using their web browsers.) The test period was from approx. 10:45 a.m. to 1:15 p.m. The httpss was used in transparent mode, (i.e. no configuration required at the desktop).

Observations

1. Achieved peak connections in the connections table of approx. 16,000 connections.

```
localhost     proxied_conns          18   3217
localhost     connections            19  15829
```

2. Achieved peak open sockets on the firewall of approx. 11,000 sockets. (2 x 5500, determined by using netstat and counting the number of entries of the VPN-1/FireWall-1's external interface IP address).
3. Performance from local test machine(s) browser was acceptable and comparably faster that the existing proxy technology.
4. CPU load on VPN-1/FireWall-1 averages approx. 99 % during the peak (100% at times) and averages approx. 75 % throughout the test.
5. The `ahttpd` process load on the CPU averaged approx. 15% per process (x 5). The first process always appeared to have a higher load, sometimes as high as 30% while the rest were down in the 15% range.
6. The first half of the test was without the WebSense rule. For the second half, the WebSense rule was added on the fly. Check a number of illegal sites, and get appropriate reject from WebSense rule.
7. Near the end of the test, approx. 1 p.m. a message appeared on the test browser "`FW-1: hostname: Cannot connect to WWW server`". This message appears numerous times in the `ahttpd.elg` log file. It is therefore assumed that other client browsers experienced this same message.
8. At about the same time, several console messages where received from VPN-1/FireWall-1: "`log buffer message queue full`". Because of the log buffer message, it was decided to reduce the

Excessive Log Grace period to 30 sec (See the SecureKnowledge Solution in the Check Point Technical Services site (ID 110022.0.1679268.2471760)), and then re-installed the policy.

9. Test ended approx. 1:15 p.m., and after change no. 8, it appeared that there were no more log buffer messages on the console. Number of connections at this time dropped to less than 10,000.
10. Note that many drops are logged and most appear to be return packets from web servers. These packets will continue for up to 10 min (default) as web server is still trying to close connection.
11. All `fw` and `httpss` processes are stable through the entire test, (no processes hanging, no core dumps etc.) .

Discussion

Re: observation no.4 and no. 7:
It was deemed necessary by the test team to increase the resources required for this environment. With the CPU at 99% during peak and sometime at 100%, there appeared to be no room for higher loads. Also, with the high number of "`Cannot connect to www server`" entries in the `ahttpd.elg` log file, it was determined that the box was out of resources periodically, even though this message could appear for other reasons including servers that does not respond, etc.

Re: observation no. 8:
After reducing the Excessive Log Grace Period to 30 sec, (half the default of 60 sec.), the messages to the `console "Log buffer message queue full"` stopped. This message occurs when the kernel process responsible for the logging is filling the buffer for the log messages faster than the user mode process can empty this buffer This is a normal message identifying the potential loss of important log messages. A better remedy is a faster CPU and /or to increase the size of the log queue, which is a system parameter. The latter may in some cases not resolve the problem.

Re: observation no. 10:
These are mostly late packets from the web server(s) as determined by a network sniffer. Because the connection has already been removed from the connections table, (i.e. client browser has already closed or reset its connection to the transparent proxy) these packets are dropped by the clean-up rule. Possible remedy is to increase `:tcpendtimeout` from 50 sec to some higher value. This will allow the connection to stay in the connection table longer and therefore allow the packets to get through and therefore get ack'd and the connection to be closed in an orderly fashion. This has a negative side effect of drastically increasing the size of the connections table.

Another solution is to add a rule to filter these return packets, from any, source port 80, to the external IP address of VPN-1/FireWall-1 on port gt. 1023, reject, no track. This will at least eliminate these from the log viewer. This was determined to be the preferred corrective action for this environment.

Another solution is to make a code change to enable Check Point gateways to drop non-first TCP packets instead of matching the rule base. It should be noted that this INSPECT fix will cause a change of behavior from the existing Check Point gateway behavior in the following way. Following a reboot, policy unload or stopping the FireWall, all active TCP connections will be blocked, and any timed-out TCP connections (i.e., connections that have been inactive longer than the TCP timeout) will be disconnected. The ability of VPN-1/FireWall-1 to maintain connections after policy reload will not be affected by this change.

For the changes, see http://www.checkpoint.com/techsupport/alerts/ackdos_update.html

Once these connections have been removed from the connections table, these packets will be dropped by rule 0 – so this might explain these kind of log messages.

Action Plan

Following this test, the following actions were taken. They are presented for the purpose of illustration, and may be a useful guide for your own environment.

1. Obtained an E450, 4 CPU machine with a total of 1 GB of RAM.

2. Installed Solaris 2.6 and harden according to customer specs.
3. Installed VPN-1/FireWall-1 4.1
4. Tuned the parameters including `/dev/hme, /dev/tcp`, file descriptors, and VPN-1/FireWall-1 parameters described above.
5. Increased the number of instances of the `httpss` to between 8 and 10.
6. Modify the Rule Base to eliminate the logging of legitimate drops.
7. Set the Excessive Log Grace Period to 30 sec.
8. Run a production test to determine performance during peak load.

Conclusions

Following this test, the following conclusions were drawn. They are presented for the purpose of illustration, and may be a useful guide for your own environment.

1. The resources required for this environment need to be increased in order to achieve a level of performance that does not completely exhaust VPN-1/FireWall-1 and OS resources and provides some margin for future growth.
2. Overall the test was successful, the VPN-1/FireWall-1 product and the httpss transparent security server processes were stable and as reported periodic lack of resources as they should.
3. The performance of VPN-1/FireWall-1 and the `httpss` security servers with the enhanced feature of UFP is better (faster) than an existing proxy technology albeit on a larger and faster platform.
4. At some point, assuming growth in demand for the `httpss` service, the load will reach the limit of resources available on an E450/4 CPU machine with 1 GB of memory. Assuming there is no feasibly larger single box to go to, the only option at this point would be one of load balancing.

Resolving Common HTTP Security Server Problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base http://support.checkpoint.com/kb/index.html.

VPN-1/FireWall-1 Security server and HTTP 1.1

There are two known problematic features in HTTP 1.1, which is not supported by the VPN-1/FireWall-1 HTTP versions 4.0 and 4.1 security server.

Chunk transport encoding with content inspection

The HTTP server can send its response in a chunked mode. That means that the body of the request will include headers and footers from some of the chunks. The HTTP 1.1 client knows how to parse the body and extract the data. The security server knows how to parse the body but in VPN-1/FireWall-1 versions 4.0 and 4.1 it does not know how to clean the body before it passes it to the content inspection modules (e.g. CVP server html weeding). If the content inspection module is not aware of the headers and the footers, it is possible that it will not be able to recognize suspicious data patterns, such as virus patterns. In VPN-1/FireWall-1 versions 4.0 and 4.1 the security server will block any chunked responses if the connection was matched on a rule with content inspection. To allow this connection, some attributes must be added to the `objects.C` file, the `props` section.

```
:http_cvp_allow_chunked (true).
:http_weeding_allow_chunked (true).
:http_block_java_allow_chunked (true).
```

Another instance of this problem is the range request. The client can ask the server to send just part of the response. It can do it by adding the range request header. In that way the smart client (Trojan horse) can get the second half first and then get the first half. The HTTP security server will block each range request unless the user will add the `http_allow_ranges` to the `props` section of the `objects.C` file.

Multi-server connections to an HTTP Security Server acting as Security Proxy

The HTTP 1.1 protocol supports multi-request connections, where each connection can carry more than one request/response transaction. An example of a multi-request connection is a connection to a single page where different elements of the page reside on different servers.

Where the HTTP security server is in proxy mode, the client can open a single connection to the proxy and send the proxy a number of requests where each request has a different server as a final destination. The proxy is supposed to handle all the requests, send each request to the right destination and return the response to the client. In this scenario therefore, a single connection from the client to proxy relates to many connections between the proxy and the servers. As of VPN-1/FireWall-1 4.0 and 4.1 the HTTP security server does not support this feature yet. It supports only one request/response transaction per connection, so that every server requires its own connection.

To work around this problem, whenever the VPN-1/FireWall-1 HTTP Security server gets a request where the final destination differs from the destination of the previous request (on this connection), it will try to respond with a redirect and will close the connection. This workaround does not always work because some of the HTTP client will not follow the redirect.

Another workaround:

Disable the support for multi request connections. In this case, the security server will enforce only one request for each connection.

You can add the following attributes to the `props` section of the `objects.C` file.

`:http_avoid_keep_alive (true)`
closes the connection after the first request/response transaction.

`:http_force_down_to_10 (true)`
changes the version of the protocol from 1.1 to 1.0.

See the SecureKnowledge Solution (Solution ID: 10022.0.2181016.2491988) in the Check Point Technical Services site.

Client Authentication issues related to the HTTP Security Server

Problem with Partially and Fully Automatic HTTP Client Authentication

Note: This issue is documented in the Check Point 2000 Administration Guide page 554

Packet Flow description

When the kernel has match on a partially automatic HTTP client authentication rule, it folds it to the security server. The security server returns a redirection response, which forces the HTTP browser to open second connection to the redirected URL. In this case, the new URL is the VPN-1/FireWall-1 security server. The security server manages the authentication process and adds a new entry to the client authentication table. It then returns a redirection response, which directs the browser to the original URL. The browser opens new connection to the original URL, but this times it passes through the FireWall using the new client authentication table entry.

The problem

The redirect response includes two major headers: the action header, which has the return code (e.g. HTTP/1.0 302 Not Allowed), and the location header, which direct the browser to the new URL (e.g. Location: http://199.203.71.111/index.html).

The browser prints the URL in its address window (the one which the user uses to enter the requested URL), and after getting a redirect response it replaces the original URL with the one from the location header. A URL contain two parts: the host name and the path. A transparent HTTP request does not include the full URL but only the path (so that if the user enters http://www.checkpoint.com/index.html the HTTP request will include only the "/index.html" part).

The effect of all this is that when VPN-1/FireWall-1 redirects the browser back to the original URL, it puts the IP address in the location header instead of the host name which is not available, which in turn causes the browser to replace the URL with the IP address.

Solution

When using Partially or Fully Automatic Client Authentication, it is now possible to configure the VPN-1/FireWall-1 so that the redirection sent to the client that points it to the server, will be done according to the host header and not according to the destination IP.

To enable redirection according to the HTTP host header, follow these steps:

1. On the management station, issue the `fwstop` command (or on NT stop the VPN-1/FireWall-1 service)
2. In the file `$FWDIR/conf/objects.C`, under the line which includes the token
   `:props (`

   Add the following line:
   `:http_use_host_h_as_dst (true)`
3. Start the FireWall by running `fwstart` (on NT, start the VPN-1/FireWall-1 service).

Session Authentication Rules and Domain objects

If the connection matches a rule in which the source field contains Domain objects or the Action is Session Auth., the rule will not apply, and the connection will probably be rejected by the stealth (Any/Any/Drop) rule.

Agent Automatic Sign On

Agent Automatic Sign On is a new feature in VPN-1/FireWall-1 4.0 SP5 and 4.1 SP1. Since it operates the Session Authentication mechanism for all services, including Authenticated services such as HTTP, FTP etc., you are not allowed to configure on the same rule a URI resource (FTP, SMTP, HTTP) or any kind of Security Server. Automatic Sign On does not have this restriction

HTTP Security Server and DNS

For related solutions, search the SecureKnowledge database http://support.checkpoint.com/kb in the Check Point Technical Services site

Performance Issue: VPN-1/FireWall-1 defined as a proxy in the client's browser

Where VPN-1/FireWall-1 is not defined as a proxy the DNS query is done by the client. However, if the VPN-1/FireWall-1 is set as a proxy, the destination of packets sent by the client will always be the IP of the VPN-1/FireWall-1 machine. Therefore in this case VPN-1/FireWall-1 has to issue DNS query for each HTTP request passing through the HTTP Security Server. DNS queries are very time consuming, which could degrade HTTP Security Server performance.

URI Resource – In the Match tab the Host field contains URL name

In order for the VPN-1/FireWall-1 Security Server to be able to do match on that specific rule which contains a URL name in the host filed of the match tab of the URI Resource, it has to do a Reverse DNS lookup for each HTTP request.

In case it fails the connection will be dropped and the client will be notified with a message "Unknown WWW server" or "The WWW server is not responding".

How to use CVP for content security with HTTP and/or a URI service on ports other than 80

1. First set up VPN-1/FireWall-1 to invoke the HTTP Security Server to send Port 80 traffic to the CVP Server.
2. Define the CVP Server according to the instructions in the VPN-1/FireWall-1 Administration Guide.
3. Define a Resource of type "URI" according to instructions contained in the VPN-1/FireWall-1 Administration Guide, and be sure the "Host" field on the "Match" tab is
   :
   (asterisk, colon, asterisk)
4. Create a Rule with appropriate Source and Destination and specify the Service as "http-->Resource"

If other ports are specified in a URL, and the CVP server must inspect the traffic for content, then:

1. Create a User_Defined TCP service of type "URI" and specify the port to be used.
2. Create a Rule with appropriate Source and Destination and specify the Service as "User_Defined-->Resource"

See the SecureKnowledge Solution (ID: 36.0.1952321.2504884) in the Check Point Technical Services site

What rules are needed when setting up Content Security

A rule allowing a connection from the FireWall to the CVP server on port 18181 for the control connection is needed. The Rule also needs to allow TCP high ports between the firewall and the CVP server. This is for the file transfer from the FireWall to the CVP server for inspection of the file.

Rules that specify CVP inspection do not replace rules that allow FTP, HTTP, or SMTP connections. Since VPN-1/FireWall-1 examines the Rule Base sequentially, you must define rules in the appropriate order to prevent unwanted traffic from entering your network.

Resource rules that accept HTTP, SMTP, and FTP connections must be placed before other rules which accept these services. If you define a rule that allows all HTTP connections before a rule that specifies CVP inspection on a URI Resource, you may be allowing unwanted traffic.

Similarly, CVP rules must be placed after rules that reject FTP, HTTP or SMTP Resource connections. For example, a rule rejecting large email messages must come before a CVP rule allowing specific SMTP connections.

See the SecureKnowledge Solution (ID: 36.0.608403.2485073) in the Check Point Technical Services site

Troubleshooting Security Server Performance problems

Where there are problems with the HTTP security server and attempts to troubleshoot the problem have been unsuccessful, it is worth testing the configuration to determine which object is responsible for the slowing down and blocking of the HTTP security CVP servers, and the reason why.

It is also possible to generate debug information that can be sent to Check Point Support for analysis.

The following test plan was developed for a scenario where, the HTTP security server with a WebSense CVP server on a loaded network slowed down or became blocked, while other connections worked well.

Test Plan

Diagram of the Environment

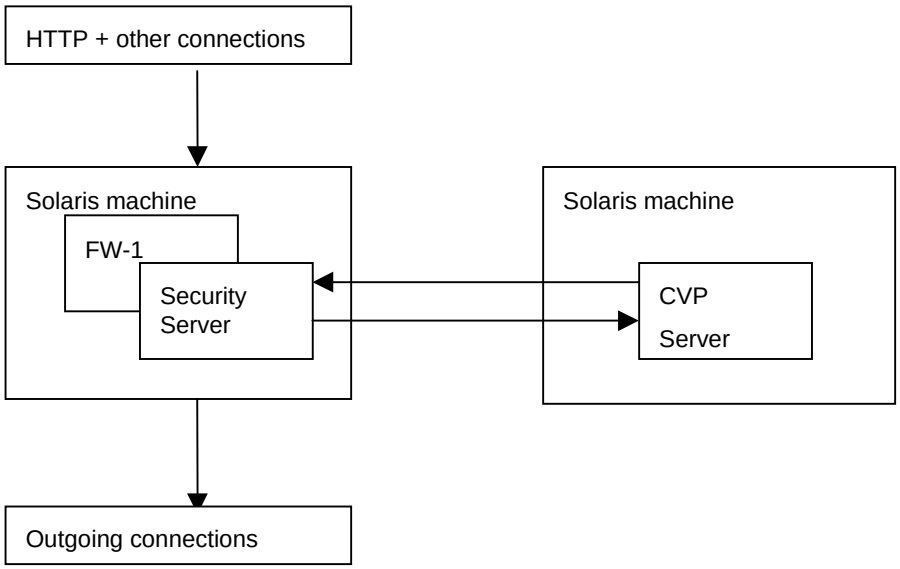


Figure 1. Test environment for solving Security Server performance problems

The environment involved the following objects: 2 Solaris machines, a VPN/FireWall module, HTTP security servers, and a CVP server.

Requirements for the test

1. Separate the VPN-1/FireWall-1 and CVP servers.
2. Monitoring tools like: top, snoops, logs or accounts, and easy access to the objects involved

What are the possible causes?

It is worth defining the possible causes of the problem. Assume that every one of the involved objects can be a cause of the problem, and that the problem may arise from a combination of causes.

Possible causes for each object:

The Solaris machines

1. Overloaded CPU
2. Memory problem
3. Running out of File descriptors

The VPN/FireWall module

1. Limitation of kernel tables
2. A loaded kernel blocking the security servers

The security servers

1. A general security server bug
2. A security server with a CVP/UFP resource bug
3. CVP server saturation.

The CVP server

1. A bug

The test

Start with a low load, and then build up to a higher load. Either start the tests at a quiet time or divide the load on the security and the CVP servers via the Rule Base.

1. Run all the following measurements before starting

   `top`
   for CPU and memory usage on both machines,

   `lsof (lsof | grep <process name> | wc –l)`
   for file descriptors checks, on both machines

   `fw tab –s`
   for the firewall kernel tables counts.

   `Snoop`

   Save the log and `ahttpd.log` files.
2. Turn the CVP resource on and start the measurements again. Look for changes.
3. If you see nothing unusual, increase the load by performing the test at a busier period.
4. If you see the problem or its symptoms, determine the cause. See the above list of possible causes.

Test Results

From the tests you should be able to determine:

1. The faulty object. From now on you can be more focused in your resolution.
2. A measurement of the load (accounts, logs, snoops) and the network view (snoops).
3. The state of the machine resources.
4. The VPN-1/FireWall-1 and/or CVP server limitation/bug.

FTP Security Server

In this section

This section describes the permitted FTP security server commands, and how to solve common problems

"The FTP security server," page 66

"Resolving Common FTP security server problems," page 66

The FTP security server

The FireWall-1 FTP security server is optimized for security. Several FTP commands that could present risks are therefore not implemented:

- `SOCK` commands – commands that allow the user to open sockets (tunneling)
- `SITE` commands – commands that allow the user to send special commands to the ftp server by using the site resources.
- `MAIL` commands – commands that allow the user to send and use e-mail through ftp.

In addition to these security enhancements, the FTP Security Server provides protection from port spoofing by not allowing the opening of ports to an IP address that is different from the one used to connect.

All though not recommended, it is possible to allow the usage of all of those commands listed above, which FireWall-1 by default prohibits.

To allows those commands, create a file called `aftpd.conf` in the `$FWDIR/conf` directory and edit the following lines:

- `Optimist` allows the passage of unlisted commands.
- `sock_cmd` allows SOCK commands to be issued.
- `port_spoof` allows opening ports to different IPs.
- `site_cmd` allows SITE commands to be issued.
- `mail_cmd` allows mail operations to be used.

Resolving Common FTP security server problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base (http://support.checkpoint.com/kb/index.html)

FTP data connections are dropped by the FireWall

Problem Description

- FTP data connections are dropped by the FireWall
- Error received in the info field of the log viewer
- Error: 'reason: tried to open tcp service port, port: <service name>'
- FTP Data connections reject on Rule 0FTP data connections are dropped by the FireWall

Fix

There are several things you can do to alleviate this.

1. Delete the FireWall-1 service(s) that are causing the problem. This is the easiest solution, but is not always feasible.

   (Pre-defined high-port TCP services are listed below).

2. Delete the FireWall-1 service(s) that are causing the problem, and recreate them as a service type of 'Other'. That way FireWall-1 will not see them as known TCP services. Please see this link for information on how to do this: How to manually define a TCP port range

3. Perform a base.def modification to keep FireWall-1 from comparing against these known services. Always back up any file before modifying it, and make sure you use a UNIX based editor such as VI to edit this file. NT editors place carriage return / line feeds at the end of the text. If you are using the `base.def` on an NT machine, use edit.com from the command prompt rather than Notepad or Wordpad.

Make this modification on the Management server to `your $FWDIR/lib/base.def`. then stop/start the FireWall, and re-install the Rule Base.

Original `base.def`:

```
// ports which are dangerous to connect to
define NOTSERVER_TCP_PORT(p) {
      (not
          (
             ( p in tcp_services, set sr10 RCODE_TCP_SERV, set sr11 0,
              set sr12 p, set sr1 0, log bad_conn)
          or
             ( p < 1024, set sr10 RCODE_SMALL_PORT, set sr11 0, set sr12
p,
              set sr1 0, log bad_conn)
          )
      )
};
```

is changed to:

```
// ports which are dangerous to connect to
define NOTSERVER_TCP_PORT(p) {
      (not
          ( p < 1024, set sr10 RCODE_SMALL_PORT, set sr11 0, set sr12 p,
           set sr1 0, log bad_conn)
      )
};
```

you need to re-install the policy for the changes to take effect.

List of pre-defined high-port TCP services:

1235	vosaic-ctrl	
1352	lotus	
1494	Winframe	
1503	T.120	(NetMeeting)
1521	sqlnet	
1525-1526	sqlnet2	
1570-1571	Orbix	
1720	H323	(iphone)
1723	pptp	
1755	NetShow	
2000	OpenWindows	
2049	nfsd-tcp	
2299	PCtelecommute	

2626	AP-Defender,	AT-Defender
2649,2651	IIOP	
2998	RealSecure	
5190	AOL	
5510	SecurID-prop	
5631	PCanywhere	
6000-6063	X11	
6499	IS411	
6660-6670	IRC	
7000	IRC2	
7070	RealAudio	
12468-12469	WebTheater	
16384	ConnectedOnline	
18181-18184	CVP, UFP, SAM, LEA	
18187	ELA	

See the SecureKnowledge Solution (ID: 47.0.707710.2521144) in the Check Point Technical Services site

Allowing FTP data connections through the FireWall on random ports

VPN-1/FireWall-1 by default assumes data connection coming from port 20.

See the SecureKnowledge Solution (ID: 10022.0.714865.2422686) in the Check Point Technical Services site

Port command must end with a new line

VPN-1/FireWall-1 expects to receive the PORT command with /r/n at the end

You can change this behavior by changing the INSPECT code.

See the SecureKnowledge Solution (ID: 36.0.152763.2473228) in the Check Point Technical Services site

Bi-directional FTP Data connection are not allowed

Unlike the FTP Control connection that is a bi-directional connection, the DATA connection is unidirectional. One side sends ACK packets and the other side sends DATA packets. VPN-1/FireWall-1 always forbids bi-directional commands because they are considered to be insecure.

FTP servers that allow bi-directional FTP connections allow FTP data connections from random ports on FTP servers.

VPN-1/FireWall-1 imposes unidirectional data transfer on connections opened via the port or the PASV command in the FTP protocol

Fast mode and FTP

Since VPN-1/FireWall-1 has to inspect each packet in order to understand the port command and thereby opens only the relevant port for the data connection, FAST mode is not supported with FTP.

See the SecureKnowledge Solution (ID: 10000.0.1236618.2339349) in the Check Point Technical Services site

FTP connections hang during large file transfers

It appears that when a packet comes through that is just a little bit less than the MTU size, the FireWall will accept it. But then the FireWall adds it's data to the packet, which makes it larger than the MTU threshold and it is dropped. The packet is resent and is accepted and then dropped again for the same reason. This becomes an endless loop and the connection appears to freeze.

Reducing the MTU on the FireWall should help the situation. The FireWall will then require the server to fragment the packets into smaller pieces, avoiding this problem. If the application does not allow fragmentation of the packet, then it will not work with encryption.

See the SecureKnowledge Solution (ID: 33.0.241016.2462650) in the Check Point Technical Services site

FTP PASV vulnerability:

The FTP PASV vulnerability arises when the parsing of FTP control connections by VPN-1/FireWall-1 is manipulated via the MTU. An FTP server PASV port number, as processed by VPN-1/FireWall-1, is associated with the port number of a service with a known security issue (such as a ToolTalk port vulnerability on an un-patched Solaris 2.6 system). This enables the client to exploit the server's vulnerability (i.e., an in.ftpd that returned client-controlled data in an error message and running a possibly unnecessary service: ToolTalk) to gain root access on the machine.

This vulnerability was reported to BugTrack on Wednesday, February 9th, 2000 by John MacDonald of DataProtect.

For a solution http://www.checkpoint.com/techsupport/alerts/pasvftp.html

PORT command is blocked

If the FTP security server is active you may encounter the problem in which the PORT command is blocked although you have modified the macro NOTSERVER_TCP_PORT in the base.def file

To overcome this, do the following

1. Add the following line to the `:props` section of the `$FWDIR/conf/objects.C` file on the management station
   `:ftp_dont_check_random_port (true)`
2. Configure file name `aftpd.conf`

See the SecureKnowledge Solution (ID: 10022.0.2917673.2504701) in the Check Point Technical Services site.

FTP commands being blocked by the FTP Security Server

When issuing one of the following commands "`get`", "`put`"," `delete`", "`mkdir`" or " `rename`", the FTP security server issues a `PWD` command in order to get the full path and put it in the log. The FTP server responds to the "`PWD`" command with a "`257`" message, which according to RFC 959 must contain the absolute path in quotes. When the path is not put in quotes (as required by the RFC), the command entered by the user will be blocked by the FTP Security Server.

See the SecureKnowledge Solution (ID: 10022.0.123051.2372308) in the Check Point Technical Services site.

PWD command is not enabled on the FTP server

When the FTP security server is enabled, while issuing the following commands "`get`", "`put`"," `delete`", "`mkdir`" or "`rename`", the FTP security server issues a `PWD` command. Therefore `PWD` command should be enabled on the server otherwise the connection will be dropped.

See the SecureKnowledge Solution (ID: 3.0.143507.2194044) in the Check Point Technical Services site.

The FTP Security Server has problem getting to sites which start with number such as 3ftp.3com.com. This should be fixed in FireWall-1 4.0 SP7

10043.0.5311843.2582690

How to cross several VPN-1/FireWall-1 Authentication Daemons

See the SecureKnowledge Solution (ID: 3.0.114740.2192532) in the Check Point Technical Services site.

How to add a support for a new command to the ftp security server

The following commands are supported by ftp Security Server

```
ABOR, ACCT, ALLO, APPE, BYE, BYTE, CDUP, CWD, DELE, FIND, FW1C, HELP, LIST,
MACB, MAIL, MDTM, MKD, MLFL, MODE, MRCP, MRSQ, MSAM, MSND, MSOM, NLST,
NOOP, PASS, PASV, PORT, PWD, QUIT, REIN, REST, RETR, RMD, RNFR, RNTO,
SITE, SIZE, SOCK, STOR, STOU, STRU, SYST, TYPE, USER, XCUP, XCWD, XMD5,
XMKD, XPWD, XRMD.
```

To force the security server to allow other- possibly unsafe- commands…

See the SecureKnowledge Solution (ID: 10022.0.2917673.2504701) in the Check Point Technical Services site.

SMTP Security Server

In This Section

This section describes the SMTP email and security server processes, how to troubleshoot VPN-1/FireWall-1 SMTP Security Server problems, error handling and the solutions to some common problems.

"SMTP Email Process," page 71

"The SMTP Security Server Process," page 72

"Troubleshooting Common SMTP Security Server problems," page 73

"Understanding the error handling mechanism of the SMTP daemon," page 74

"How SMTP Security Server deals with envelope format," page 75

"Log Viewer Error Messages," page 75

"What commands are supported by the VPN-1/FireWall-1 SMTP Security Server?," page 77

"More Information: Security servers and content Security," page 79

SMTP Email Process

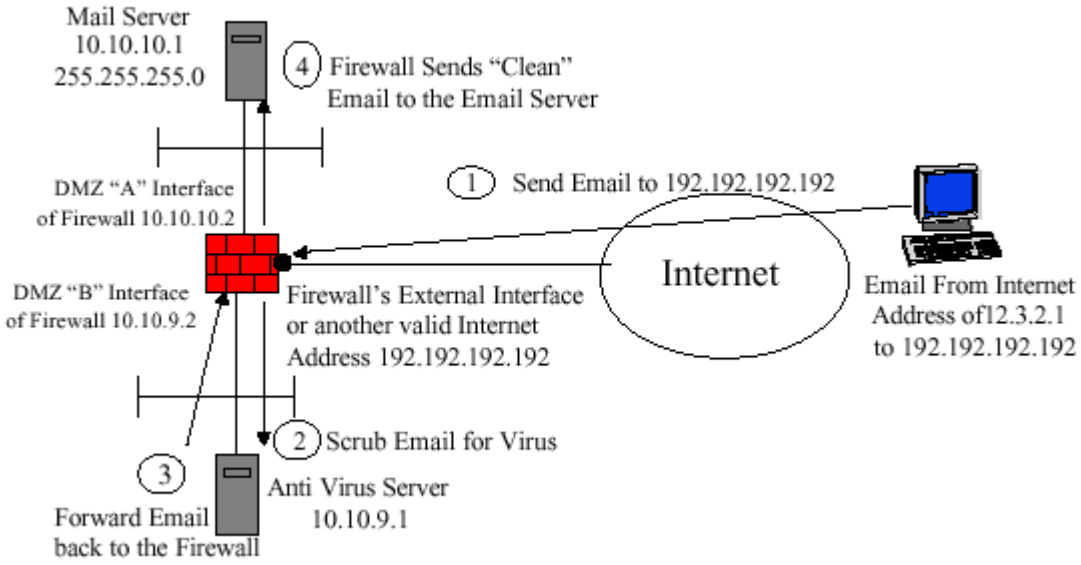


Figure 2. The SMTP Email process. Follow the numbers…

The SMTP Security Server Process

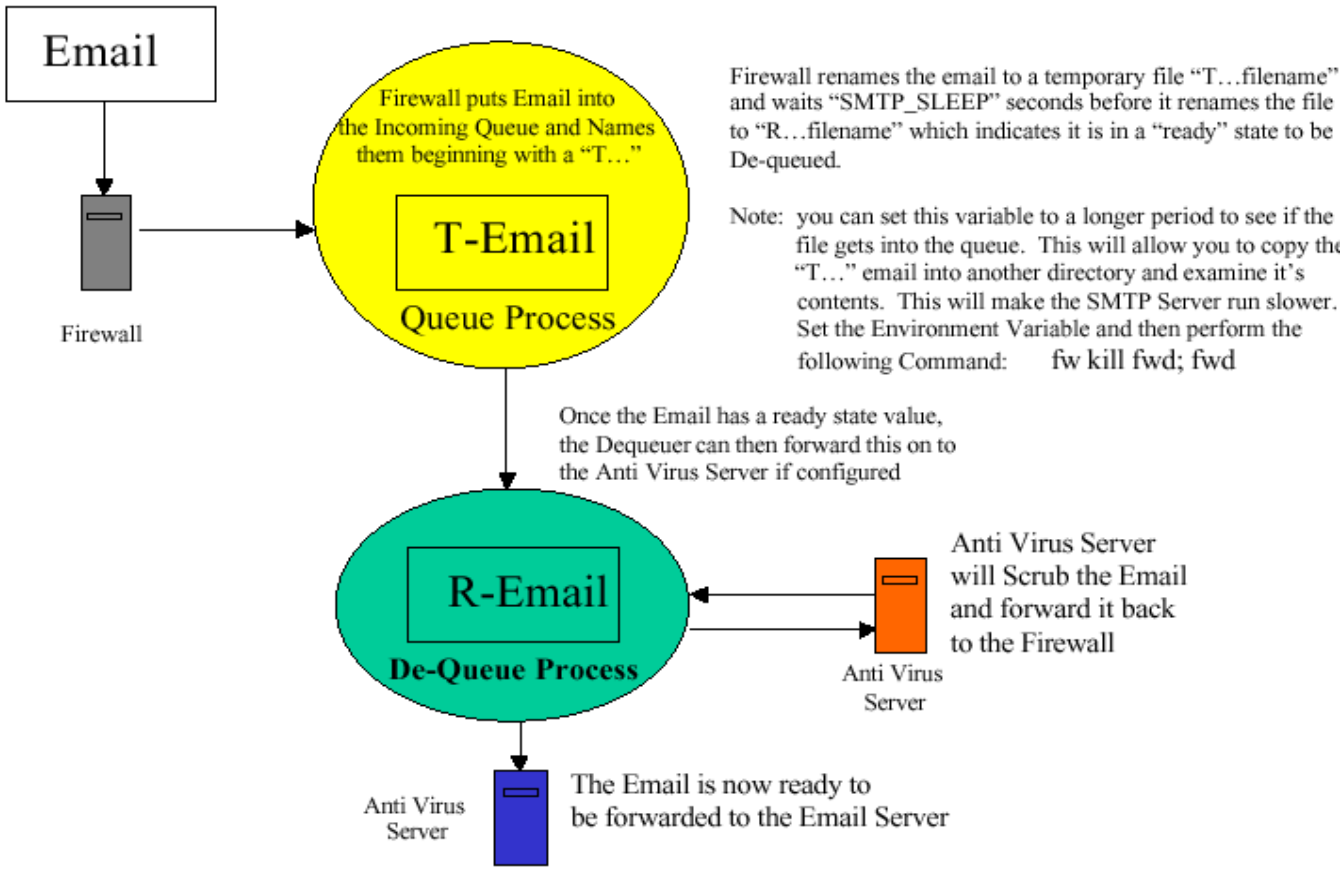

Email
Firewall puts Email into the Incoming Queue and Names them beginning with a "T…"
T-Email
Queue Process
Firewall
Firewall renames the email to a temporary file "T…filename" and waits "SMTP_SLEEP" seconds before it renames the file to "R…filename" which indicates it is in a "ready" state to be De-queued.
Note: you can set this variable to a longer period to see if the file gets into the queue. This will allow you to copy the "T…" email into another directory and examine it's contents. This will make the SMTP Server run slower. Set the Environment Variable and then perform the following Command: fw kill fwd; fwd
Once the Email has a ready state value, the Dequeuer can then forward this on to the Anti Virus Server if configured
R-Email
De-Queue Process
Anti Virus Server will Scrub the Email and forward it back to the Firewall
Anti Virus Server
Anti Virus Server
The Email is now ready to be forwarded to the Email Server

Figure 3. SMTP Security Server - flow of events

When using the VPN-1/FireWall-1 SMTP Security Server, a certain flow of events takes place from the time the user sends the message, to the time the message arrives to the actual mail server:

1. The user composes the message, and sends it through the SMTP Client to the original server (the user is not aware of the fact that a VPN-1/FireWall-1 SMTP Security Server is in place).
2. The VPN/FireWall inspection module intercepts the SMTP connection, and decides that the request should be sent to the Security Server. The connection is folded into the Security Server.
3. The VPN-1/FireWall-1 SMTP Security Server receives the folded connection and checks, in the appropriate rule's resource how to handle the connection and performs the necessary actions (rewriting, mime stripping…).
4. After all the necessary actions performed the message is transferred to the spool directory waiting for the mail dequeuer.
5. The mail dequeuer examines the spool directory for messages.

   Three types of messages can be put in the spool directory. The initial letters of the files distinguish them: T, R, E.

   - T stands for Temporary file, which is a file not yet fully received.

- R stands for Ready file, which is a file that is ready to be sent on.
- E stands for Error file, a file that cannot be sent for some reason and needs to be processed.

6. The SMTP Security Server receives a file that starts with T and turns it into an R type.
7. The dequeuer takes the R file and sends it on, or processes it into an E file.
8. The mail dequeuer opens a new connection to the final SMTP server and to the CVP server (if requested).
9. If CVP connection requested, the mail dequeuer receives the file back from the CVP server and completes the session by sending the message to the final SMTP server.

Troubleshooting Common SMTP Security Server problems

SMTP Security Server problems may arise in three places:

1. Connection between the Email Client and the VPN-1/FireWall-1 SMTP Security Server
2. Connection between the VPN-1/FireWall-1 Mail Dequeuer and the Anti Virus Server
3. Connection between the VPN-1/FireWall-1 Mail Dequeuer and the Final Email Server

Connection between the Email Client and the Firewall SMTP Security Server fails

To troubleshoot the connection between Email Client and the VPN-1/FireWall-1 SMTP Security Server:

1. Look in the Log Viewer to see if the email connection is accepted from the appropriate rule in the Rule Base. Also check the 'Info' column of the Log Viewer. This is where the connection is described in more details (see “Appendix C: Log Viewer "info" Messages,” page 189).
2. Make sure the email has completed the queuing process and has a name of T#### (where ### is the email order number, given by VPN-1/FireWall-1) under the spool directory. This is located under the default installation directory of:

   `\winnt\fw\spool` for Windows NT
   `/etc/fw/spool` for UNIX

3. If there is no file in this directory after the email has been sent by the Client, and the log file displays that the SMTP connection has been accepted, make sure the SMTP Security Server has been configured correctly. Validate this by running the following:

   `\winnt\fw\bin\fwconfig` for Windows NT
   `/etc/fw/bin/fwconfig` for UNIX

   Make sure the SMTP Security Server is defined to start with the other VPN-1/FireWall-1 Security Servers. This will place a "`asmtpd`" entry into the directory:

   `\winnt\fw\conf\fwauthd.conf` for Windows NT
   `/etc/fw/conf/fwauthd.conf` for UNIX

   If this entry does not exist add the following line to the `fwauthd.conf` file:

   ```
   25   in.asmtpd   wait   0
   ```

4. Run TELNET to the Mail Server on port 25 to see if the SMTP Security Server works. Enter the command "help" or "?" to see VPN-1/FireWall-1 SMTP Server replies.

See the SecureKnowledge Solution (ID: 10022.0.1775714.2480161) in the Check Point Technical Services site

Connection between the Firewall Mail Dequeuer and the Anti Virus Server fails

Troubleshoot the connection between the VPN-1/FireWall-1 Mail Dequeuer and the Anti Virus Server as follows:

1. Make sure VPN-1/FireWall-1 can ping the Anti Virus Server
2. If this is successful, then see if the Anti Virus software has received an email from the VPN-1/FireWall-1. This will tell you if the VPN-1/FireWall-1 has accepted the email from the Client, queued it, renamed the email and forwarded this on to the Anti Virus Server.
3. Validate that the Proper CVP ports are configured on the Anti Virus Machine and the VPN-1/FireWall-1 Resource. By default the parameter `FW1_cvp` uses port 18181.
4. Run TELNET to the mail server on port 25 to see if the SMTP Security Server works. Enter the command "help" or "?" to see the VPN-1/FireWall-1 SMTP Server replies.
5. Use a packet sniffer, or the "snoop" command in UNIX or the Network Monitor Agent in NT to see if there is any communication between the VPN-1/FireWall-1 Dequeuer and the Anti Virus Machine.

See the SecureKnowledge Solution (ID: 10022.0.1775726.2480161) in the Check Point Technical Services site

Connection between the Firewall Mail Dequeuer and the Final Email Server fails

Troubleshoot the connection between the VPN-1/FireWall-1 Mail Dequeuer and the Final Email Server as follows

1. Make sure VPN-1/FireWall-1 can ping the Final Email Server
2. Try and use the SMTP Resource without the Anti Virus Server being defined. Now download the Security Policy to the VPN-1/FireWall-1 again and see if the Email passes from the Queuer to the Dequeuer and then on to the Final Email Server. If the above works correctly, then the problem lies with the Anti Virus Server. Please refer to “Connection between the VPN-1/FireWall-1 Mail Dequeuer and Anti Virus Server fails”
3. Try and TELNET from the VPN-1/FireWall-1 to the Final Email Server on port 25 to see if a connection can be made. This will show if the SMTP process on the Email Server is configured and active, so that the Dequeuer can forward the email to the Final Email Server.

See the SecureKnowledge Solution (ID: 10022.0.1775733.2480161) in the Check Point Technical Services site

Understanding the error handling mechanism of the SMTP daemon

When configuring an SMTP resource, the Firewall administrator can decide to notify the sender by setting the “Notify Sender On Error” button and specify the “Error Handling Server”.

When an error occurs, i.e. a message was sent to a non-existent user, the sender of the mail will be notified by e-mail that the transaction failed, and the reason for that failure (the user sending this notification is the one defined as postmaster in the smtp.conf file).

At the same time the message is transferred to the error handling server that will try to send it through its own channel (the error handling server is supposed to be a fully qualified smtp server).

How SMTP Security Server deals with envelope format

The envelope format is:

```
Mail from: sender
Rcpt to: recipient
```

However if there are multiple recipients the envelope format is:

```
Mail from: sender
Rcpt to: recipientA
Rcpt to: recipientB

…
Rcpt to: recipientN
```

VPN-1/FireWall-1 SMTP Security Server examines the first "Rcpt to" in the envelope, and matches the resource according to what it finds. When it deals with multiple "rcpt to" which don't all match the same resource, the VPN-1/FireWall-1 gets "confused" and rejects the mail.

See the SecureKnowledge Solution (ID: 10022.0.2918688.2504663) in the Check Point Technical Services site

Log Viewer Error Messages

I. Error: "450 Mailbox Unavailable"

Using the following policy:

Table 1: Error: "450 Mailbox Unavailable" Policy

Rule:	Source:	Destination:	Service:	Action:	Track:
1.	any	mailserver	smtp->foo	accept	long
2.	any	mailserver	smtp->baa	accept	long
3.	any	any	any	drop	long

foo is a resource that matches all emails to foo.abc.com.

baa is a resource that matches all emails to baa.xyz.com.

If a single email is sent that specifies fred@foo.abc.com and fred@baa.xyz.com, the SMTP Security Server returns "450 Mailbox Unavailable" and fails to deliver the message.

Solution: This is not a VPN-1/FireWall-1 bug. It is however a limitation of VPN-1/FireWall-1. These errors arise when one mail is matched by two resources, and each resource demands different behavior from the mail. This is very different from sending the same email to one recipient at a time, since in this case it is matched on only one resource. It is therefore necessary to send separate emails to the two different destinations.

At this time the VPN-1/FireWall-1 cannot treat more than one resource at a time in the same rule. Also once something has been passed through one rule it cannot be checked against another rule.

See the SecureKnowledge Solution (ID: 10043.0.4138283.2569517) in the Check Point Technical Services site

II. Error: "554 Mailbox unavailable" when trying to deliver mail

Cause: The added SMTP Resource does not allow that type of mail to be delivered

Solution: The FireWall SMTP daemon answers a mail client with an "554 Mailbox unavailable" error message when the loaded policy handles mail with SMTP recourses. It does not allow that type of mail.

See the SecureKnowledge Solution (ID: 3.0.132201.2193912) in the Check Point Technical Services site

III. Error: "agent mail server ... reason: Too much mail data" in the Log Viewer

Cause: The size of sent email was larger then maximum mail size that is configured in the mail resource

Solution: Increase max email size in the SMTP Definition > Action2 > Don't accept Mail Larger Than:

See the SecureKnowledge Solution (ID: 10043.0.6566373.2619870) in the Check Point Technical Services site

IV. Error: “Connection to Final MTA failed”

Solution: Decrease the value of the following variables in $FWDIR/conf/smtp.conf file

a) max_load (default 40, 4.0SP3 and later)

This value is an abstract measure for the load generated by the mail dequeuer while emptying the mail-spool. It corresponds to the number of messages mdq will attempt to deliver at one time using the following formula:

```
max_load = 2x + 4y
```

where

x is the number of connections that do not involve CVP
y is the number of connections that do involve CVP

Example:

```
max_load = 60
```

If mail goes through CVP, then the max is 15 emails.
If mail doesn't go through CVP, then the max is 30 emails.

The parameter can be set as high as 60. On Solaris and HP, it can be set to 100. If the value exceeds this limit, the mail dequeuer will not run. This option should be used to adjust the load that the mail dequeuer generates to the load that can be handled by the peer mail server. When the mail dequeuer generates more load than the peer mail server can handle, the peer mail server might refuse the mail dequeuer's connection attempts, possibly causing mails to accumulate in the mail dequeuer's spool, and delaying delivery. This parameter's value should be set according to the load capacity of the main peer mail server.

b) resend_period (default 600)

Number of seconds after which the SMTP Security Server resends the message after failing to deliver the message. If the CVP server has a high load, you could increase this parameter. If the load is on the firewall, this parameter can be decreased.

c) timeout (default 900)

Increase the number of seconds after which the connection times out. This includes the amount of time VPN-1/FireWall-1 will spend on CVP scanning a message and delivering it to the final MTA (Mail Transfer Agent). This value should be at least 900 seconds, if not longer.

See the SecureKnowledge Solution (ID: 33.0.235874.2462444) in the Check Point Technical Services site

What commands are supported by the VPN-1/FireWall-1 SMTP Security Server?

Solution: The commands that are supported are the basic SMTP commands. VPN-1/FireWall-1 does not currently support the ESMTP command structure. The commands that are offered by the Security Server are:

```
HELO  MAIL  RCPT  DATA  RSET  NOOP  QUIT  HELP
```

See the SecureKnowledge Solution (ID: 47.0.1261642.2525193) in the Check Point Technical Services site

Debugging Security servers

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

This section lists the information that Check Point Support will ask you to gather in order to debug security Server problems. It may also be of use when doing your own troubleshooting.

See “Chapter 2: Troubleshooting Tools,” page 5 for more information on the `fwinfo, fw monitor` and the `fw ctl debug` commands.

Information to Gather

HTTP Security Server

To debug the HTTP Security Server, do the following:

1. Issue the f`wstop` command, or `fw kill fwd`
2. `Setenv FWAHTTPD_DEBUG=1`
3. f`wstart` or `fwd`

The debug output will be redirected to file `ahttpd.elg` (or `ahttpd.log` in pre-4.1 version)

Send the files to support@ts.checkpoint.com.

Authentication

Gather the following information:

1. `fwinfo` file.
2. Error messages from the log and from the screen.
3. `fw monitor` file that is relevant for the problem.
4. Send the `log/ahttpd.log` file to support@ts.checkpoint.com.
5. If the problem is related to SMTP, ask for the spool directory and run the mail dequeuer and the `asmtpd` in debug mode.

Send the files to support@ts.checkpoint.com.

Resources and CVP servers

Gather the following information:

1. `fw monitor` on port 18181.
2. `fwopsec.conf` file.
3. `cvp.conf` file on the CVP side.
4. Set the environment variable `OPSEC_DEBUG_LEVEL` to 3, and restart `fwd`. Send the output received in `fwd.log` to support@ts.checkpoint.com.

More Information: Security servers and content Security

- VPN-1/FireWall-1 4.0 Architecture and Administration User's Guide

  Chapter 2: Security Servers
  Chapter 3: Content Security

- VPN-1/FireWall-1 4.1 and 4.1 SP1 (Check Point 2000) Administration Guides

  Chapter 11: Security Servers and Content Security

Chapter 8: Troubleshooting LDAP Servers and the AMC

In This Chapter

Introduction 81

LDAP problems 81
Introduction to Account Management 81

Troubleshooting LDAP Issues 82

Installation Issues 83

Account Management Client Installation 83

Configuration Issues 83

Configuring an LDAP Server for VPN-1/FireWall-1 Indexing 83
Schema Checking 84
Ensuring compatibility between the AMC and the specific LDAP server 84
VPN-1/FireWall-1 LDAP Server Communication 85

Known configuration problems 85

AMC Configuration problem 86

Working with the AMC 87

Before Starting the Account Management Client 87
The Organizational Unit 87
Deleting an Organizational Unit 87
Creating a Tree Object 88
Modifying `slapd.conf` (on the LDAP Server) 88
Defining Users 88
The LDAP server 88
When do the changes take effect? 88

Working with LDAP 89

Managing LDAP through the command line 89
Working with 3rd party LDAP Servers: `fw ikecrypt` 89

Known LDAP and AMC problems 89

AMC cannot read synchronized groups 89
Exporting Users Problems 90
Problems while initiating a connection 90
Problems while working with OPSEC LDAP Servers 90

Special Configurations 91

Multiple LDAP Servers 91
Known Issues between LDAP and Meta IP 91

PKI Issues related to LDAP 91

Known Limitations 92

Debugging LDAP 93

Important Debugging Tools 93
fw ldapsearch 94

More Information 95

Troubleshooting LDAP Servers and the AMC

Introduction

This document contains useful information about LDAP Servers and the VPN-1/FireWal~1 Account Management feature.

To implement the VPN-1/FireWal~1 4.1 Account Management module, you must install and configure three components:

- FireWall-1
- An LDAP server containing users, groups and templates information
- Account Management Client (AMC)

The following information will help you debug and troubleshoot each component.

Note – For important information about how LDAP is used in VPN-1/FireWal~1, see "VPN-1/FireWall-1 LDAP Account Management" in Chapter 5, "Managing Users" of VPN-1/FireWall-1 Administration Guide.

LDAP problems

LDAP problems can be divided into these categories:

1. AMC problems
    - Installation
    - GUI
    - Problems while using the AMC.
2. VPN-1/FireWall-1 related issues
3. LDAP related issues
    - Installation
    - Limitations
    - Known problems

This document covers the first two categories. Since the installation category is specific for each type of LDAP Server, you should consult the documentation accompanying the LDAP Server.

Introduction to Account Management

Account management for a large network can be a daunting task. Maintaining synchronized user databases is a time consuming chore. Organizations that have multiple user databases in one firewalled network can appreciate a process where all databases are maintained from one location.

VPN-1/FireWall-1 allows such a process through the use of the Account Management Client.

Security engineers can define and maintain databases with the Account Management Client (AMC) using the Lightweight Directory Access Protocol (LDAP). The Account Management Client is an independent module used to integrate an LDAP server with VPN-1/FireWall-1 user authentication.

Note – For important information about how LDAP is used in VPN-1/FireWall-1, see "VPN-1/FireWall-1 LDAP Account Management" in Chapter 5, "Managing Users" of the VPN-1/FireWall-1 Administration Guide.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is used to communicate with a server that maintains information about users and items within an organization. LDAP is the lightweight version of the X.500 ISO standard. Each LDAP server is called an "Account Unit."

Three features of LDAP are as follows:

- LDAP is based on a client/server model in which an LDAP client makes a TCP connection to an LDAP server.
- Each entry has a unique distinguished name (DN).
- Default port numbers are 389 for a standard connection and 636 for a Secure Sockets Layer (SSL) connection.

Distinguished Name

A globally unique name for an entry, called a distinguished name (DN), is constructed by concatenating the sequence of DNs from the lowest level of a hierarchical structure to the root. The root becomes the relative DN. This structure becomes apparent when setting up the Account Management Client (AMC), which manages multiple user databases in one firewalled network.

Example

If searching for the name John Brown, the search path would start with John Brown's CommonName (CN). You would then narrow the search from that point, to the organization he works for, to the country. If John Brown (CommonName) works for the ABC Company, one possible DN might be:

"`cn=John Brown, o=ABC Company, c=US`"

This can be read as "John Brown of ABC Company in the United States".

A different John Brown who works at the 123 Company might have a DN as follows:

`"cn=John Brown, o=123 Company, c=UK"`

The two common names "John Brown" belong to two different organizations with different DNs.

The Account Management Client (AMC)

To look for information in an LDAP server, or to change it, administrators need a graphical user interface (GUI).

All of the major LDAP Server comes with their own GUI. Check Point provides the Account Management client as a graphical user interface to manage VPN-1/FireWall-1 specific object attributes over LDAP.

Most LDAP clients include only the standard LDAP fields. Check Point has its own requirements from a user database.

Troubleshooting LDAP Issues

The LDAP Server configuration consists of several components, which must work together properly. The primary problem is to identify the component that causes the failure.

The problem could reside at the AMC, the LDAP, VPN-1/FireWall-1 or even at the SR client, which initiate the connection. The most important step is to identify the failure location. There are few steps, which you can follow in order to find this failure.

1. Test the connection without SR client, and with users defined in the VPN-1/FireWall-1 database. If the problem consists then it is not related to the LDAP server or to the SR.

- Choose Manage Users and define a default user.
- In the policy editor, enter a user authentication rule.
- Test the connection.
- If the problem persists, then it is not related to the LDAP server.

2. If the problem disappeared, try to initiate a “user authentication action” rule with users defined on the LDAP.
3. If the problem disappeared, then it might be a SR or encryption issue.
4. If you have reached this point, then the problem is probably LDAP related, and this document should help you solve it. Try to locate the log files on the LDAP, which may contain error messages that indicate the cause of the problem.

Installation Issues

Refer to the LDAP Server’s user guides for information on how to install the LDAP Server, and follow the instructions carefully.

Account Management Client Installation

Important: Only AMC builds 140 and above are Y2K compliant.

The Account Management Client can be installed on Windows 9x and Windows NT (Intel only).

If you are updating an older version of the Account Management Client to AMC builds 140 or 142, a message will appear asking whether you would like to update all the objects on the current Account Unit. For more information on updating your Account Units, see the Check Point Account Management Client Build 140 Release Notes at http://www.checkpoint.com/support/technical/documents/index.html.

Please note that this is relevant to AMC builds 140-142 and may change in the future.

Configuration Issues

In order to properly configure the Account Management Module, the administrator must be familiar with the following:

- LDAP
- configuring an LDAP server
- configuring the VPN-1/FireWal~1 GUI
- configuring the Account Management GUI

The first goal is to enable a user defined in an LDAP Server to authenticate to the VPN/FireWall Module using a fixed password. After this modest goal is achieved, you can undertake something more complex.

See: How to integrate Account Management and Netscape LDAP Server v3.1 with VPN-1/FireWall-1 (Solution ID: 55.0.4222079.2607206) in the Check Point Technical Services site.

Configuring an LDAP Server for VPN-1/FireWall-1 Indexing

As mentioned in the User Guide, to maximize an LDAP Server’s performance, it is recommended to index the LDAP Server according to the following attributes:

- DN
- UID

- Member
- objectclass

These indexes reduce lookup time, but there is a trade-off between faster lookup times and the extra disk space needed to store the additional indexes. (See Known limitation for search related issues).

Schema Checking

The LDAP schema is a description of the structure of the data in an LDAP directory.

Each LDAP should have instructions regarding the way to set the VPN-1/FireWall-1 Schema.

When schema checking is enabled, LDAP requires that every object class and its associate's attributes be defined in the directory schema.

When you first begin to use VPN-1/FireWall-1 Account Management, you should confirm that schema checking is enabled (you can check the error logs to see if there is anything wrong with the schema).

Each LDAP has its own way of setting the VPN-1/FireWall-1 schema. Schema configuration issues are the most frequently encountered LDAP issues.

See the following Solutions in the Check Point Technical Services site

- How to access the FireWall-1 LDAP schema (Solution ID: 55.0.1120086.2568794) in the Check Point Technical Services site
- See instruction for how to set the VPN-1/FireWall-1 Schema on NDS

See the following solutions for VPN-1/FireWall-1 Schema Issues in the Check Point Technical Services SecureKnowledge:

- How to use LDAP without implementing the VPN-1/FireWall-1 Schema on the LDAP Server? (Solution ID: 10043.0.460391.2521903

For more configuration issues, see the following solutions:

- Is filter used by VPN-1/FireWall-1 when searching the ldap directory for user groups adjustable? (Solution ID: 10043.0.5520134.2585567)
- How to create a new Netscape LDAP Server on Netscape LDAP 3.x? (Solution ID: 10022.0.1178630.2444127)

This applies to AMC version AMC127 and above.

Ensuring compatibility between the AMC and the specific LDAP server

You may need to edit the `AMC.properties` file, in order to ensure compatibility between the AMC and the specific LDAP server.

The following properties are defined in the `AMC.properties` file located in the `Properties/CheckPoint/Account Management/` directory.

Table 1: AMC.properties

AMC Property	Meaning

AMC Property	Meaning
GroupRequiresMember=TRUE	This variable is set to FALSE by default, and groups are created without members when they are defined. However some servers force the groupOfNames type by disallowing empty group. Setting this variable to TRUE will create the group with a dummy member.
UserDefaultOC= person | organizationalPerson | inetOrgPerson | fw1person	On some servers, there may be problems with these values. When creating a new userobject, the objectclasses types will be taken from this variable. Also, when editing an existing user (any subset will be considered as user), all the missing objectclasses will be added. However, they will be added while editing only if the AddUserDefaultOC is TRUE.
AddUserDefaultOC=TRUE	This variable tells the AMC whether to add the default objectclasses to any user object being edited. On some servers (e.g. NDS) the objectclass cannot be changed while editing.

To get the defaults, you need to delete the old `AMC.properties` file, since there is still no update mechanism for this file. The AMC creates an `AMC.properties` file with the default values if it cannot find it.

More Information

For more information about Account Management Client, see the Check Point Account Management Version 1.1 User Guide.

VPN-1/FireWall-1 LDAP Server Communication

For securing the communication between VPN-1/FireWall-1, an AMC and an LDAP Server, you can choose between three alternatives:

- If the LDAP Server is SSL-enabled, the VPN-1/FireWall-1 and the AMC can use SSL to communicate with the LDAP Server.
- Use a VPN for the communication.
- Put the LDAP Server inside a network protected by VPN-1/FireWall-1

Note – The VPN-1/FireWall-1 User Database always has priority over Account Unit. It is recommended that you define the network and system administrators as VPN-1/FireWall-1 users, so that they will always be able to log in to the VPN-1/FireWall-1 Management Station, even if the LDAP connection is down.

Known configuration problems

Problem: Account Management Client Authentication Error, while launching the AMC from the policy editor.

When system administrators try to view the contents that were entered in the AMC and in the LDAP Server, they may receive an authentication error regarding the administration server. This error means the Netscape LDAP Server has not been set up completely.

Solution:

1. Enter the directory manager's password in the SuiteSpot settings.

2. Confirm the administrator's name and password. This establishes communications between the LDAP and administration server.

Do not change the administrator's name or password. The previous step is done to establish communications between the LDAP Server and the Administration Server.

Problem: What are the restrictions for the LDAP parameters in the VPN-1/FireWall-1 properties?

Answer: There are two configurable parameters in the properties, the defaults are in parentheses:

- Time-out on LDAP requests – this cannot be larger then the TCP timeout (20)
- Time out on cached Users (900)
- User Cache Size (1000)
- Password expiration in days (90)
- Allowed number of Entries which the Account Units returns (10000)

Except for the Time-Out on LDAP requests, there are no restrictions on these values.

You should note that:

- During installation of policy, the system cleans the cached memory.
- Most of the servers allow similar definitions on the server side. E.g. size limit could be configured to 100 on the server's side and 10000 on VPN-1/FireWall-1. The actual size would be the minimum (100) in this case.
- There was a bug which caused the 'time out on cached users' to be ignored, while the value was larger then 900 seconds, and the user authenticated with certificates, this bug has been fixed in VPN-1 4.1 SP2 and VPN-1 4.0 SP6. (for more information see PKI Issues related to LDAP on page 91).

AMC Configuration problem

Problem: If the AMC cannot connect to the LDAP server from within VPN-1/FireWall-1, then check one of the following:

- Account Unit definitions in VPN-1/FireWall-1 are not correct. Check the login and password fields in the Account Unit window.
- LDAP server is not up, check that the 'service' is running.
- LDAP server is not configured correctly.
- Check that the "login DN" you have configured has root permission or at least write permission in the access control configuration of the server.
- Check that there are no special configurations to block the AMC from whom you are working in the access control configuration of the server.

When you create a new user on the LDAP Server using the AMC, the name you enter in the "Login Name" field will be the login name to use when authenticating to VPN-1/FireWall-1.

Make sure there is no other user with the same login name.

Working with the AMC

Before Starting the Account Management Client

The LDAP Server must be running in the background before starting the AMC. The server and AMC must bind with each other before being able to talk to one another.

Before starting the AMC, you must do the following:

1. Confirm that Use LDAP Account Management is checked in the Security Policy GUI Properties Setup window LDAP tab.
2. Confirm that User Management is checked on the Account Unit's General tab.
3. Check that the LDAP server is accessible from the VPN/FireWall Module machine (e.g. no rule prevents the access, routing, etc.)
4. Confirm that there is a VPN-1/FireWall-1 workstation object with the IP address of your LDAP server.
5. Confirm that there is a VPN-1/FireWall-1 server object for an LDAP server using the LDAP Account Unit.
6. In Login DN (Account Unit's General tab), use the same logon DN that you created when you created the Netscape LDAP server (`cn=loginname`…). Note that the DN is case sensitive.

You may need to edit the `AMC.properties` file, in order to ensure compatibility between the Account Management Client and the particular version of the LDAP server. (See Ensuring compatibility between the AMC and the specific LDAP server on page 84,).

The Organizational Unit

An organizational unit is created to hold lists of users, groups and templates. After connecting to the LDAP server, the AMC shows organizational units, users, groups, and templates to exist as part of the LDAP database. Likewise, if users and organizational units are created in the LDAP server itself, they will also appear in the AMC.

Warning: `"ou="` is implied. Do not type it. If you type it (for example, `"ou=Accounting"`), then the organizational unit's name will include `"ou="` (for example, `"ou=ou=Accounting"`).

Deleting an Organizational Unit

You cannot delete an organizational unit using the AMC. You must use the `ldapmodify` utility, as follows:

To delete the organizational unit from the AMC:

1. Start the appropriate command-line interface.
2. Locate `ldapmodify.exe` (Windows) or `ldapmodify` (Solaris).
3. Enter the following command at the prompt:

   ```
   ldapmodify -h <host> -d "<login DN>" -w <bind password>
   ```

   `ldapmodify` will wait for input statements terminated by CNTRL`-D`.

4. To delete a branch, enter the following statements with this syntax (The `ou` object can be any DN starting with `ou`):

   ```
   dn: ou=name,o=name
   ```

```
changetype: delete
```

`control-d` to end the input

5. The following message appears:

   ```
   deleting entry ou=name,o=name
   ```

6. Close and restart AMC to reflect the changes.

Creating a Tree Object

If a “X” overlies a node in the tree, then one of the following conditions is true:

- It is defined in the `slapd.conf` file (on the LDAP Server) with the suffix parameter, but it does not exist in the LDAP directory.
- It is defined as a branch in the Account Unit, but is not defined in `slapd.conf` with the suffix parameter.

In the first case, you can create the object in the LDAP directory by:

- Right-clicking on it and choosing Create this Object from the menu, or
- Selecting it and choosing Create Tree Object from the File menu.

In the second case, the object cannot be created with the Account Management Client, because it must already be present in `slapd.conf`.

Modifying `slapd.conf` (on the LDAP Server)

The `slapd.conf` file usually contains definitions of the root branches. You can modify the `slapd.conf` file in two ways:

- using any text editor
- using your LDAP Server’s configuration utility

Defining Users

Before creating a user, group, or organizational unit, be certain that Schema Checking is enabled. (Regarding the VPN-1/FireWall-1 schema see Schema Checking, on page 84.

Problem: Cannot create LDAP groups with the AMC (Account Management Client), while using the New Group icon (Solution ID: 10043.0.6499710.2614415) in the Check Point Technical Services site.

Workaround: Use the title bar, choose File New Group

The LDAP server

Important: Both VPN-1/FireWall-1 and LDAP user databases cache users, so any change in the users definition will take effect after policy installation or cache timeout.

For example, if you delete a user from a group and only install the User Database, that user will still be allowed access under Client Authentication rules.

When do the changes take effect?

If you make changes using the AMC, your changes will effect VPN-1/FireWall-1 only after one of the following happens:

- The cache times out.
- The Security Policy is installed.
- The user database is downloaded.

Working with LDAP

Managing LDAP through the command line

If the AMC is not available, or if it has not been installed, you can manage the LDAP directory from a remote terminal, using the command line. This option is also helpful in order to debug LDAP failures, for more details, see:

How to create users on an LDAP server from a remote terminal? (Solution ID: 10022.0.1178639.2444127) in the Check Point Technical Services site.

How to get the list of users that is defined on the LDAP server? (Solution ID: 10022.0.1178646.2444127) in the Check Point Technical Services site.

Working with 3rd party LDAP Servers: `fw ikecrypt`

On FireWall-1 4.0 SP5 and VPN-1/FireWall-1 4.1 SP1, the `fw ikecrypt` command was added to the fw command line. This command can be used to generate an IKE shared secret that can be used by a 3rd party LDAP users management tool.

Syntax

```
fw ikecrypt [SecretKey] [UserPassword]
```

Options

Table 2: fw ikecrypt options

parameter	meaning
`SecretKey`	A secret string stored in the Account Unit that the user belongs to.
`UserPassword`	A string that will be used by the user to log in.

The output will be the encrypted secret to place under the "`fw1ISAKMP-SharedSecret`" user attribute. This is also useful for writing bulk scripts for LDAP (with LDIF format).

Known LDAP and AMC problems

AMC cannot read synchronized groups

Through the use of the Netscape Directory Synchronization Service (LDAP Server version 4.1) one can load all NT users and groups into the LDAP database.

By enabling LDAP in Policy Properties, correctly defining an account unit server object, and defining an external group to use this server, VPN-1/FireWall-1 can authenticate using the synchronized users and their associated passwords. VPN-1/FireWall-1 will also correctly restrict access based on the NT group if "Only Group in Branch" is selected as part of the external group's scope definition.

On AMC versions (below build 140) there was a problem with the AMC reading the synchronized groups (and the user associations), in the LDAP database. Even though the NT groups appear in the Netscape "Users & Groups" console window, they do not appear in the AMC.

The AMC could not recognize the attributes "`uniquemember`" or the objectclass "`groupofuniquenames`" The AMC was looking for attributes of "`member`" and objectclass "`groupofnames`" instead.

Solution:

1. Upgrade to AMC build 140 and above. AMC build 140 and above support both `groupOfNames` and `groupOfUniqueNames`. You can view these groups with different color and you can add/remove members. There is no need to manually modify the group types (this might have negative effects on Netscape).
2. If you are using an older AMC version, in order for the AMC to see the group definitions and the users in those groups, you must make modifications to the user attributes for the group and the objectclass.

Exporting Users Problems

You can export users from the VPN-1/FireWall-1 internal user database to an LDAP directory by using the `fw dbexport` command. (For further information, see "Exporting a User Database" in page 41 of Check Point 2000 Reference Guide.

See the SecureKnowledge solution: How to export a user database? (Solution ID: 47.0.3358861.2547129) in the Check Point Technical Services site

Problems while initiating a connection

Problem: User not found.

Solution:

1. Make sure that Use LDAP Account Management in the LDAP tab of the Properties Setup screen is checked.
2. Using the Account Management Client, verify that the user is indeed defined in the Account Unit.

Problem: VPN-1/FireWall-1 rejects the user's password.

Solution: This might happen if the user is defined differently in the VPN-1/FireWall-1 user database, or in an Account Unit with a higher priority.

Check the Display user's DN at login field in the LDAP tab of the Properties Setup window and try again. The user's DN will be displayed, and you will know from where VPN-1/FireWall-1 is getting the user's password.

Problems while working with OPSEC LDAP Servers

Issue: Cannot delete user on NDS (BG000560)

LDAP Protocol Error (error 2 in Delete) return via the AMC

SEND_LDAP_RESULT 2::Unknown Request from the LDAP trace screen on the NDS server

Workaround:

Use another LDAP client:

- ldapdelete – ldap delete entry tool or

- ldapmodify – ldap modify entry tool.

Alternatively use Novell ConsoleOne.

See: NDS users cannot be deleted from the AMC (Solution ID: 10043.0.1133507.2535007) in the Check Point Technical Services site Fix: AMC build 142 fixed this issue.

Special Configurations

Multiple LDAP Servers

There are several advantages in using more than one LDAP server, including the following:

- Compartmentalization, by allowing a large number of users to be distributed across several servers
- High availability, by duplicating information on several servers
- Remote sites can have their own LDAP servers that contain the database, and so speed up access time

See: Are multiple account management licenses required for multiple, autonomous LDAP servers? (Solution ID: 55.0.639999.2564039) in the Check Point Technical Services site.

Known Issues between LDAP and Meta IP

Meta IP uses LDAP for mapping between machines and IP addresses.

There are a few solutions available in the Check Point Technical Services site regarding the integration of LDAP Servers with Meta IP, as follows:

Are there any LDAP issues addressed by service pack 3 for Meta IP? (Solution ID: 55.0.1500760.2572592)

How to manually replicate the LDAP directory? (Solution ID: 21.0.1533853.2440442).

Solution regarding error messages:

Error: "LDAP Error: Invalid credentials (0x31)" (Solution ID: 36.0.1900980.2504068).

PKI Issues related to LDAP

How to achieve Entrust communication between two FireWall-1 Modules and two different LDAP servers with same database? (Solution ID: 10022.0.574263.2413933) in the Check Point Technical Services site.

Problem: A user is trying to integrate Certificate Manager with Netscape LDAP 4.0, and it cannot import the ldif file.

Solution: This is a problem in Netscape. The Netscape 4.0 does not recognize the '-' character in our schema even though this is RFC compliant for schema definitions.

Netscape has already fixed this in their 4.1 beta. You can supposedly get it to work by adding the following flag in `slapd.conf`:

```
attribute_name_exceptions 1
```

Problem: LDAP Cache setting ignored when using certificates (BG000551)

Firewall is set to cache LDAP users for a longer period than 15 minutes. If SR uses Entrust certificates for authentication, then when SR reauthenticates after its 15 minute timeout, the LDAP server is queried again by the firewall rather than caching information. This causes VPN-1/FireWall-1 to not cache LDAP users with certificates per the timeout value.

Known Limitations

Performance issue when the large groups of users (more than around 1000 - 1500 users) are defined on the LDAP server (Solution ID: 10043.0.5520148.2585567) in the Check Point Technical Services site.

This limitation is related to two issues:

The VPN-1/FireWal~1 looks up for the groups the user is member in, any time the user supposed to be fetched. The query used to bring the whole group object from the LDAP.

From VPN-1 4.1 SP-2 and VPN-1 4.0 SP-6 the behavior was changed and only the group DN is retrieved from the LDAP server (this is a big difference when the group is big).

While the old implementation used to query the groups using the AU branches as search base, the new queries use the DNs of the external groups defined for each AU. For example, supposed that we have the following:

a. A single AU with `"o=cp,c=il"` as the branch

b. Two external groups based on the following LDAP groups:

   1. `cn=rndg1, ou=rnd,o=cp,c=il`
   2. `cn=supportg1, ou=support, o=cp,c=il`

The old implementation used to query the branch `"o=cp,c=il"`. The new implementation query the two branches (in LDAP any object is a valid search branch) `"cn=rndg1, ou=rnd,o=cp,c=il"` and `"cn=supportg1, ou=support, o=cp,c=il"`.

From this fix the queries do not retrieve the group content (which is very large with large groups).

This should improve the performance for the LDAP search.

The indexes the LDAP server is configured to work with (i.e. the attributes that the server make the hashing with so it can fast answer queries that include these attributes as the filter). In order to improve server performance the "member" attribute better be indexed at the server.

Debugging LDAP

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

This section lists the information important debugging tools for use when troubleshooting LDAP problems. File outputs can also be sent to Check Point Support support@ts.checkpoint.com

See “Chapter 2: Troubleshooting Tools,” page 5 for more information on the `fwinfo, fw monitor` and the `fw ctl debug` commands.

Important Debugging Tools

1. The Log Viewer – the VPN-1/FireWall-1 log file might contain informative error messages.
2. `fwenc.log` file – If SecuRemote is involved try, the `fwenc.log` file should be very informative.

   See: How to troubleshoot SecurRemote problems by creating a fwenc.log file (Solution ID: 47.0.1537649.2530505)

1 fw ldapsearch

2. `fwd.log` (the output of the `fw d –d` command).
3. Environment Variables.

   See the following SecureKnowledge solutions in the Check Point Technical Services site:

   How to set environment variables in Windows NT? (Solution ID: 36.0.92223.2471774).

   How to set environment variables on UNIX? (Solution ID: 10022.0.3099256.2509558).

4. The LDAP log files – each LDAP has its own log files, which might be informative as well (usually access and error logs).

   For example: The Netscape log files are: `access.log` and `error.log` (located in `Netscape/SuiteSpot/slapd-<serverid>/logs`

5. AMC files: `admin.lst` and `AMC.properties` located in the `Program Files/CheckPoint/Account Management` directory. These files will enable you to get the same configuration of AMC as the customer.
6. VPN-1/FireWall-1 files: `fwinfo`

   See: How to use the fwinfo utility to create and package debug information to send to Support (Solution ID: 10022.0.1592028.2468724).

7. Snoop files - If you have a Sniffer or a snoop utility, you can trace the connection between different entities and check if the connection exists.

   See: How to get a packet snoop on Windows NT Solution ID: 36.0.2503074.2514022).

fw ldapsearch

Using this function you can access the LDAP server, and get all the information it contains— including the CRL (Certificate Revocation List).

Syntax

```
ldapsearch [options] filter [attributes...]
```

where:

Filter RFC-1558 compliant LDAP search filter

attributes whitespace-separated list of attributes to retrieve

(if no attribute list is given, all are retrieved)

Table 3: fw ldapsearch attributes

Attribute	Meaning
-A	Retrieve attribute names only (no values)
-B	Do not suppress printing of non-ASCII values
-b basedn	Base dn for search
-D binddn	Bind dn
-d level	Set LDAP debugging level to `level'
-f file	Perform sequence of searches listed in `file'
-F sep	Print `sep' instead of `=' between attribute names and values
-h host	LDAP server
-l time lim	Server Side time limit (in seconds) for search
-p port	Port on LDAP server
-S attr	Sort the results by attribute `attr'
-s scope	One of base, one, or sub (search scope)
-t	Write values to files in /tmp
-T Timeout	Client side timeout for all operations. (in milli-seconds)
-u	Include User Friendly entry names in the output
-w passwd	Bind passwd (for simple authentication)
-Z	Encrypt with SSL
-z size lim	Server Side size limit (in entries) for search

Examples

On Windows NT machines, if the DN referred to is the DN of the CRL (`cn=CRL1` if CA is Entrust).

```
fw ldapsearch -h host -b "cn=CRL1, o=check point, c=IL"
certificaterevocationlist=* certificaterevocationlist
```

With a CA other than Entrust, you should mention the DN of the CA object if non-Distribution Points are mentioned.

```
fw ldapsearch -h host -b 'cn=CRL1, o=check point, c=IL'
```

```
certificaterevocationlist=\* certificaterevocationlist
```

on Solaris machines

There are also other parameters:

```
-D ‘o=Check Point, c=IL’ –w password
```

Example: to check the link with LDAP server:

```
fw ldapsearch -h host -D "o=Check Point, c=IL" -w password -b
"o=CheckPoint,c=IL" objectClass=*
```

you will get all the LDAP information.

More Information

For more information on LDAP Account Management, see:

Version 4.1 SP1

Check Point 2000 Administration Guide
Chapter 5: Managing Users, VPN-1/FireWall-1 LDAP Account Management, page 174.

Version 4.1

Administration Guide
Chapter 5: Managing Users, VPN-1/FireWall-1 LDAP Account Management, page 171.

Version 4.0

Administration Guide
Chapter 4: Account Management, page 135.

Chapter 9: Troubleshooting Active Network Management

Troubleshooting Synchronization

Synchronization and High Availability 98

Feature Not Supported by synchronization 98
What Tables are synchronized 99
Troubleshooting Synchronization 99
Synchronization Tests 99

Resolving Common Synchronization Problems 100

How to add a table to the Synchronization Tables 100
Support for High Availability for IPSec/IKE 100
How to verify the state tables on primary and secondary FireWalls are being synchronized 100
Will Synchronization work between two gateways that differ in platform? 100

Troubleshooting Fail-over

Fail-over in High Availability Applications 101

Introduction 101
High-Availability Failure Detection - How it works 101
VPN Fail-Over 103
Troubleshooting Fail-Over 103
Resolving Common Fail-Over Problems 105

Debugging High-Availability 106

Information to Gather 106

Troubleshooting Load Balancing

How Server Load Balancing Works 107

HTTP Method 107
Non-HTTP (Other) Method 107

Load Balancing Components 107

License requirement for Load Balancing 107

Load Balancing Configuration Guides 108

How to configure VPN-1/FireWall-1 with Connect Control (Load-Balance across multiple servers) 108
How to configure Connect Control and NAT for Server Load Balancing without Default Routes 108

Resolving Common Load Balancing problems 108

HTTP connections and the “Other” load balancing method 108
NAT and the “Other” load balancing method 108
If using Static NAT to associate external IP addresses with internal servers, which IP addresses should be used in the server group that is part of the HTTP logical server definition? 108
Load balancing does not work on HPUX when the web servers are on virtual interfaces 109
Connection going to the connect control address are dropped by the Stealth Rule 109

Debugging the Connect Control Module 109

Check_alive table 109
Logical Server of type “Other” using the round robin for the Load Balance does not work 110
How to change the load balancing connection time-out 110
How long does the Persistent Server Mode last? 111
How to get a connection to switch to the next server immediately after the server failed 111
Load Balancing does not work properly when using Persistent Server Mode 111
How to synchronize the logical_cache table 111
How to increase the size of the logical cache 112

Debugging the Load Balancing daemon lhttpd 112

Debugging the Server-Load Load balancing algorithm 112

How the Server Load algorithm works 112
About the Load measuring agent 112

Troubleshooting Synchronization

Synchronization and High Availability

Note: The section on Synchronization Applies to VPN-1/FireWall-1 4.1 SP1 only.

High Availability machines do not have to be synchronized. Synchronization ensures that no connections are lost when a machine takes control from a machine that has gone down. However, there are exceptions — for more information see "Restrictions" on Page 561 of the Check Point 2000 VPN-1/FireWall-1 Administration Guide. The disadvantage of Synchronization is that synchronizing internal tables on all machines reduces performance.

If you do not require synchronization, you must still configure the High Availability machines with synchronization set to no sync in the `$FWDIR/conf/sync.conf` file. If the High Availability machines are synchronized, there must be a control channel between all the machines. For a description of the `putkey` command, see "`fw putkey`" on page 12 of the Check Point 2000 VPN-1/FireWall-1 Reference Guide.

The following paragraphs are copied (with slight modifications) from the "Synchronization section on page 573 of the Check Point 2000 VPN-1/FireWall-1 Administration Guide:

There are three possible synchronization modes.

1. No synchronization
2. "Old style" synchronization (compatible with previous versions of VPN-1/FireWall-1)
3. "New style" synchronization on UDP port 8116 (compatible with the High Availability feature described in this section)

Synchronization is defined in the `$FWDIR/conf/sync.conf` file. See "FireWall State Synchronization" on page 557 of VPN-1/FireWall-1 Administration Guide

The type of synchronization is specified by the SyncMode parameter, as follows:

```
SyncMode= mode
```

where mode is one of the following values:

SyncMod Values

Value	value meaning
No sync	There is no synchronization. This is the default setting, so there is no need to change existing configurations.
TCP sync	"old style" synchronization (default value). (compatible with previous versions of VPN-1/FireWall-1). Other lines in the file specify VPN/FireWall Modules with which to synchronize.
CPHAP	"new style" synchronization on UDP port 8116. (compatible with the High Availability feature described in this section). All other lines in the file are ignored. As of VPN-1/FireWall-1 4.1 SP1 This should be used with caution. It will work properly in VPN-1/FireWall-1 4.1 SP2.

Feature Not Supported by synchronization

Features that are not included in the Kernel tables do not work over synchronized connections. The following features are not supported by synchronization:

- Content Security

- User Authentication
- Accounting

What Tables are synchronized

Not all tables are synchronized. In general, during fail-over, all the tables in the VPN/FireWall kernel that are signed with the keyword "sync" will be synchronized.

To check which tables are synchronized during fail-over, issue the **fw tab -t** <table name> command, and look for the sync keyword in the attributes line.

For example: **fw tab -t** connections

Output:

```
--------------------Connections-------------------
attributes : refresh, sync , expires 60, free function 4229871264 4, kbuf 1,
hashsize 16384
Connection = dynamic refresh

Sync expires
TCP_START_TIMEOUT
Expcall KFUNC_CONN_EXPIRE
Kbuf 1 hashsize 8192;
```

Troubleshooting Synchronization

Use fw tab to verify that entries are really synchronized.

Use fwd -d to get debugging information from the two FireWall fwd daemons.

See also “Debugging High-Availability” on page 106.

Synchronization Tests

#	Test Description	Test Configuration	Expected result	Remarks
1	Run the fw sync command between cluster machines. The fw sync function is generated after initiating the fw putkey command between the modules. To check if the fw sync is running, run the fw ctl pstat command. (fw sync is one of the components of fwd)	NT or Solaris machines in High Availability (High Availability (HA)) cluster	The sync should report no errors	
2	Run the fail-over tests (see Troubleshooting Fail-Over on page 103) with synchronization operational.	NT or Solaris machines in High Availability (HA) cluster (Primary or ACTIVE-up)	Opened connections shouldn't be lost during fail-over.	Check that the sync holds in cases of more than one concurrent fail-over.

Resolving Common Synchronization Problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

How to add a table to the Synchronization Tables

In the '$FWDIR/lib/table.def' file, search for the table that has to be synchronized, and add the string 'sync' to it.

See the SecureKnowledge Solution (ID: 10043.0.3280520.2559405) in the Check Point Technical Services site

Support for High Availability for IPSec/IKE

VPN-1 Gateway V4.1 state-table synchronization has been enhanced to handle IPSec/IKE session information, enabling high availability solutions which maintain IPSec/IKE connections during fail-over. IPSec/IKE synchronization and fail-over capabilities support both site-to-site and client-to-site VPN connections. These enhancements also enable third-party products to do load balancing between VPN-1 Gateways. High Availability solutions that leverage these capabilities are offered both by Check Point and by OPSEC partners. Note that IKE synchronization is a separately licensed (no charge) feature.

Benefits:

- Mission-critical VPN gateways are always available
- In the event of a failure, users can continue working with complete transparency

See the SecureKnowledge Solution (ID: 36.0.1469927.2500635) in the Check Point Technical Services site

How to verify the state tables on primary and secondary FireWalls are being synchronized

Run the command, "$FWDIR/bin/fw tab -t connections -s" on both FireWall modules. They should have the same number of connections if the state is being synchronized

See the SecureKnowledge Solution (ID: 55.0.6588603.2666394) in the Check Point Technical Services site

Will Synchronization work between two gateways that differ in platform?

The FireWall-1 Synchronization feature works only under the following general conditions:

- The two gateways are of the same Operating System, for instance, two NT machines.
- The two gateways have to be of the very same FireWall-1 version, including the build number. This means that, for instance, a FireWall-1 3.0b build 3064 gateway will not be able to synchronize with a FireWall-1 3.0b build 3072 machine.

See the SecureKnowledge Solution (ID: 36.0.216398.2474844) in the Check Point Technical Services site

Troubleshooting Fail-over

Fail-over in High Availability Applications

Note: The section on Fail-over in High Availability Applications Applies to: versions: 4.1 SP1

Introduction

As enterprises have become more dependent on the Internet for their core applications, uninterrupted connectivity has become more crucial to their success. Beginning with VPN-1/FireWall-1 Version 4.1, encrypted connections are supported in High Availability configurations and can survive failure of a VPN-1/FireWall-1 gateway.

VPN-1/FireWall-1 High Availability solutions consist of the following key elements:

1. A mechanism for detection of a gateway failure and redirection of the traffic around the failed gateway to a backup gateway.
2. State synchronization between two gateways, so that the backup gateway is able to continue connections that were originally handled by the failed gateway.

An important point of a High Availability (HA) firewall solution is ensuring that there is no single point of failure on the network. The primary objective of a High Availability firewall solution is providing a secure and available network 100% of the time. When a failure occurs, the redundant component(s) or back up will ensure a continuous, normal, flow of network traffic.

High-Availability Failure Detection - How it works

Internal communication between High Availability (HA) cluster machines is performed over a special protocol (FWHAP). This protocol works over UDP, but the VPN-1/FireWall-1 4.1 SP1 (Check Point 2000) implementation restricts its use to communication between machines on the same physical network. Although UDP is used, the packets are never processed by the machine IP/UDP modules but processed by the HA module before entering the machine. This allows the packets to be non-standard (such as having the same IP address both as source and destination). This is required because the protocol should allow communication between cluster machines on any interface. This includes interfaces on which cluster machines have the same IP and physical address.

The protocol uses port 8116 (both as source port and destination port), and is NOT encrypted.

Packets are sent either to a specific machine or as broadcasts.

The ether header of the packets is not standard. The source ether address (byte 6 - 11 in the packet) is not the ether address of the interface but a special ether address created by the High Availability (HA) module.

When the High Availability (HA) module is started, the cluster machines inform each other of their interface configuration (this is done over the FWHAP protocol). If conflicts are discovered in the configuration an error message is reported (to the console on Solaris and to the event viewer on NT) but no action is taken to correct this misconfiguration.

HA Cluster machine states

Every machine in the cluster reports its own state periodically and tracks the states of other machines (this is done by sending a broadcast `FWHAP_MY_STATE` packet (see the `fwha.h` file) every 0.5 seconds.

Table 1: HA Cluster machine states

State:	Explanation:
DEAD	
INIT	(In practice this is very similar to DEAD.)
STANDBY	(Possible in HA modes only, not in Load Balancing (LB) mode.)
READY	This is a transient state that should usually not last more than a fraction of a second. This state is used when a machine wants to change its state to ACTIVE. It first changes its state to READY, and when this state is confirmed by all other (not dead) machines in the cluster the state of the machine is changed to ACTIVE.
ACTIVE	The machine is filtering packets. In HA modes this means all packets. In LB mode every active machine filters some of the connections.

The state of a machine is usually determined by the machine itself (other machines only record the state reported). However, in two cases a machine may determine the state of another machine:

If machine A did not hear from machine B for more than 1 second, machine A changes the state of machine B to DEAD. Before doing so, about 0.7 seconds after machine A last heard from machine B, machine A sends FWHAP_QUERY packets, every 0.1 seconds to machine B. This means that even if the timer on machine B is not accurate, or one of the FWHAP_MY_STATE packets it sent did not reach machine A, it should not be deduced to be DEAD while still alive.

Machine A may refuse to confirm the state of machine B. This does not block machine B from being in that state but does not allow it to change to a higher state. This is usually used to block a machine from changing from READY to ACTIVE (by not confirming the READY State).

In HA mode exactly one machine should be active at a time. Two machines may never be ACTIVE at the same time. When one machine goes down and the other goes UP there may be a short period of time, typically probably no more than the round trip time between machines in the cluster, at which one machine is READY but none are ACTIV.

Except for the obvious machine failure, in which the machine cannot send any more packets (and therefore is detected as DEAD by the timeout mechanism described above), there may be other situations in which we would not like the machine to remain active (and to fail over to a stand-by machine). This is implemented by allowing problems to be reported to the HA module.

Problem Detection Devices

A problem is reported by a "Problem Detection Device" by indicating the "highest" state which this device allows the HA module to be in (i.e. DEAD < INIT < STANDBY < READY < ACTIVE). For example, when an interface problem is detected by the interface active check device (a built-in problem detection device, see Interface Active Check Device below), it blocks the state of the HA module at DEAD. When the interfaces are again OK, the interface active check device reports a blocking state of "ACTIVE" (in effect allowing all state). This does not change the state of the machine to ACTIVE. It only allows it. The machine may either be blocked by other devices or may remain in STANDBY State because another machine is active.

Interface Active Check Device

The interface active check is a built-in problem detection device that is one of the components of the HA mechanism. The cluster initiates a packet (`FWHAP_MY_STATE`) that run through the control interfaces of all the modules and checks the status of the interfaces.

Problem Notification Device (pnot)

The Problem Notification Device (`pnot`) device allows external devices to register and report problems through it to the HA module.

Problems detected by the VPN/FireWall module should also be reported using the Active Check Device Interface- for example, if the `fwd` daemon is running on each module.

How to check the modules status using the chaprob command

The `cphaprob` command may be used to register or un-register devices, to report problems, print the list of devices currently registered and the state of each device. Devices are referred to by name (this name also appears in the logs, so they should be meaningful and not too long (up to 16 characters).

The syntax of this command can be found in the Check Point 200 Administration Guide on page 575.

This interface allows reporting three states via the Interface Active Check Device (see Interface Active Check Device on page 102) (the Active Check Device): ok (= `ACTIVE`) init (= `INIT`) and problem (= `DEAD`). This interface does not allow blocking at READY or STANDBY (blocking at these states seems meaningless though the LB (Load Balancing) configuration device does block at READY).

Each machine constantly reports (in the `FWHAP_MY_STATE` message) the number of interface which it has determined to be up (it distinguishes between "inbound" and "outbound" communication). If one machine has fewer "UP" interfaces than another machine in the cluster, a problem is reported by this machine's interface active check mechanism. This means that if an interface is disconnected on all machines, no problem is detected. It should take about 2 seconds to discover an interface problem (it is preferable to lose a few packets than to fail over unnecessarily).

The interface problem detection mechanism should be able to detect "Uni-directional" problems, for example a problem on an interface that can send but not receive packets.

VPN Fail-Over

By leveraging VPN-1 state table synchronization, which includes key exchange information, Check Point's High Availability maintains IKE based VPN connections in the event of a fail-over.

VPN solutions without IKE fail-over drop all connections in the event of a failure thus forcing users to re-authenticate and re-establish connections. IKE fail-over delivers a seamless transition that is critical for many VPN deployments.

Troubleshooting Fail-Over

The High Availability cluster contains one primary module and one or more secondary modules. When the primary module fails, one of the secondary module becomes Active.

The following tests can be used to check if the failover capability is working properly, and to isolate problems if it is not. Both HA modes are tested: Primary-up mode, and Active-up mode.

In **primary-up mode** the machine with the smallest ID should, if it can, be ACTIVE. This means that if the primary machine goes down (and fails-over to the secondary machine) and then comes back up, the primary machine will again filter connections (even though the secondary machine is still functioning properly).

In **active-up mode** the machine that is currently active remains active (even when another machine in the cluster with a smaller number is OK) until this (active) machine goes down, at which point the stand-by machine with the smallest number should take over.

Note: See also "Debugging High Availability", page 106.

Interface Fail tests - Primary-up mode

#	Test Description	Test Configuration	Expected result	Remarks
1.	Disconnect 1 interface on the ACTIVE machines and reconnect it after a successful fail-over.	Cluster machines in primary-up High Availability (HA) mode.	The secondary Machine will become ACTIVE and The primary machine Dead. When the interface is reconnected the primary machine should become active again. Check that normal network traffic is restored.	This should be tested while connections are being opened between the external and internal segments.
2.	Disconnect 1 interface all cluster machines at the same time	Cluster machines in primary-up High Availability (HA) mode.	No change should occur in any of the tested machines	
3.	Disconnect all the interfaces of the ACTIVE machine at the same time and then reconnect them	Cluster machines in primary-up High Availability (HA) mode.	The secondary machine should become ACTIVE and filter connections, when the primary machine is reconnected the secondary machine should immediately change state to STAND-BY	Check that no connections are lost
4.	Disconnect 1interface from the primary machine, then 1interface from the secondary, plug back (primary first) and try the opposite.	Cluster machines in primary-up High Availability (HA) mode.	The Active machine should be the one with the most interfaces and lowest serial number at any given moment.	

Interface Fail tests - Active-up mode

#	Test Description	Test Configuration	Expected result	Remarks
1.	Disconnect \1 interface on the ACTIVE machines and reconnect it after a successful fail-over.	Cluster machines in Active-up High Availability (HA) mode.	The secondary Machine will become ACTIVE and the primary machine Dead. When the interface is reconnected the primary machine should change its state to STAND-BY. Check that normal network traffic is restored.	This should be tested while connections are being opened between the external and internal segments.
2.	Disconnect 1 interface in all cluster machines at the same time	Cluster machines in Active-up High Availability (HA) mode.	No change should occur in any of the tested machines	
3.	Disconnect all the interfaces of the ACTIVE machine at the same time and then reconnect them	Cluster machines in Active-up High Availability (HA) mode.	The secondary machine should become ACTIVE and filter connections, when the primary machine is reconnected the secondary machine should remain ACTIVE and the primary change state to STAND-BY.	Check that no connections are lost

#	Test Description	Test Configuration	Expected result	Remarks
4.	Disconnect 1interface from the primary machine, then 1interface from the secondary, plug back (secondary first). Try the opposite.	Cluster machines in Active-up High Availability (HA) mode.	The active machine should be the one with most active interfaces and remain so even if a machine with a lower serial number has the same amount of active interfaces.	

Resolving Common Fail-Over Problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

Whenever the primary returns to service it does not take over as the primary machine

The cause for this is that the "Return control to the highest priority ready machine" box, is not checked on both the primary and the secondary modules.

To fix this, check the "Return control to the highest priority ready machine" box, on both the primary and the secondary modules.

Sometimes Whenever the primary returns to service it does not take over as the primary machine – even though the High Availability tab has been set correctly for the primary *and* "Return control to the highest priority ready machine" is checked in NT or primary is set to primary-up in Solaris. This issue is presently under investigation

See the SecureKnowledge Solution (ID: 55.0.6797869.2673485) in the Check Point Technical Services site

How to address external interfaces for High Availability for Automatic Failover

External interfaces must have identical IP addresses for High Availability (HA) to work properly.

See the SecureKnowledge Solution (ID: 47.0.1736725.2532249) in the Check Point Technical Services site

Debugging High-Availability

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

Listed here is the information that Check Point Support will ask you to gather for Debugging High-Availability problems. It may also be of use when doing your own troubleshooting.

See “Chapter 2: Troubleshooting Tools,” page 5 for more information on the `fwinfo, fw monitor` and the fw ctl `debug` commands.

Information to Gather

1. fw monitor file that is relevant for the problem.
2. `fwinfo` file from management and both modules.
3. `sync.conf` file on both sides.
4. Network topology.
5. Issue the command
   `fw tab –u –t  connections > file`
   on both VPN-1/FireWall-1 machines at the same time (connections may be replaced by any other table that should be synchronized but isn’t).

Send the files to support@checkpoint.com.

Troubleshooting Load Balancing

How Server Load Balancing Works

Load Balancing allows several servers in one network to share and distribute the load among themselves while being protected by VPN-1/FireWall-1. This reduces the load to any one server and helps the security engineer manage network traffic from VPN-1/FireWall-1.

The following explanation summarizes how load balancing works. It is based on the explanation in the VPN-1/FireWall-1 Administration Guide.

HTTP Method

6. A client initiates an service request (for example, an HTTP session) to the logical server.
7. VPN-1/FireWall-1 determines which physical server will be the server for this session, on the basis of the load balancing algorithm.
8. VPN-1/FireWall-1 redirects the connection to the load balancing daemon (lhttpd).
9. lhppd direct the communication to the proper physical server, and notifies the client that subsequent connections should be directed to the IP address of a server, rather than the IP address of the logical server.
10. The remainder of the session is conducted without the intervention of the load-balancing daemon.

Non-HTTP (Other) Method

1. A client initiates a service request (for example, an FTP session) to the logical server.
2. VPN-1/FireWall-1 determines which physical server will be the server for this session, on the basis of the load balancing algorithm.
3. VPN-1/FireWall-1 statically translates the destination IP of incoming packets.
4. The reply packet is routed back through the gateway and translated back to its original state.

Load Balancing Components

Load Balancing involves three components. One way of troubleshooting load balancing is to look at each component separately

- **Connect Control Module**:
  Sits in the VPN/FireWall kernel module (See “Debugging the Connect Control Module” on page 109)
- **Load Balancing daemon (lhttpd):**
  Is the user mode process that handles HTTP requests, when the load balancing method is set to HTTP (see HTTP Method, on page 107 and “Debugging the Load Balancing daemon lhttpd” on page 112)
- **Load Balancing algorithm:**
  One of five (see “Debugging the Server-Load Load balancing algorithm” on page 112, and the VPN-1/FireWall-1 Administration Guide)

License requirement for Load Balancing

To use Load Balancing, the VPN-1/FireWall-1 license must contain the `connect` string. (Use the `printlic` command to view the license)

Load Balancing Configuration Guides

How to configure VPN-1/FireWall-1 with Connect Control (Load-Balance across multiple servers)

See the configuration document How to Configure VPN-1/FireWall-1 With Connect Control (Load-Balance across multiple servers (ID 55.0.2061878.2576947) in the Check Point Technical Services SecureKnowledge site (6 pages).

How to configure Connect Control and NAT for Server Load Balancing without Default Routes

See the configuration document Connect Control with Address Translation (ID 55.0.2061723.2576947) in the Check Point Technical Services site (4 pages).

Resolving Common Load Balancing problems

This section lists some common problems and solution, mostly from the Check Point Technical Services SecureKnowledge knowledge base.

HTTP connections and the “Other” load balancing method

A problem may arise if the OTHER method is chosen for HTTP connection. Since this method uses the NAT mechanism, each connection is handled separately and therefore every connection can be redirected to different server.

This may be a problem when user fills in few HTTP Forms, where a single HTTP server needs to handle all the data.

NAT and the “Other” load balancing method

If using Other as the load balancing method (see Non-HTTP (Other) Method, above) NAT is activated in the inbound direction.

If also applying a DST Static rule on the same physical server, in some cases it won’t be possible to perform load balancing. This may lead to unexpected results.

The reason for this is that the Connect Control module does DST Static NAT on the inbound direction. Therefore, if a DST Static NAT rule is applied as well, the DST IP address will be translated twice– the first time on the inbound direction because of the Connect Control, and again on the outbound because of the NAT rule.

If using Static NAT to associate external IP addresses with internal servers, which IP addresses should be used in the server group that is part of the HTTP logical server definition?

If using Static NAT to associate external IP addresses with internal servers, use the external IP addresses in the server group that is part of the HTTP logical server definition. The HTTP logical server will use the HTTP redirect to assign the client to a physical server. The client now directs its packets to the routeable IP Address of the physical server. If the physical server is actually hidden, then the client must be provided with the valid, external IP address that maps to the physical server through Static NAT.

Load balancing does not work on HPUX when the web servers are on virtual interfaces

No solution available at this time

See the SecureKnowledge Solution (ID 10043.0.3487758.2562155) in the Check Point Technical Services site.

Connection going to the connect control address are dropped by the Stealth Rule

If Firewall's external address is used for the Connect Control address (that is, the address to which Internet users will connect) and there is a Stealth Rule (that is, Any / Any / Firewall / Drop / Alert), this will also block the Connect Control connections from Internet users.

You may want to use another address in the valid external range for the Connect Control address and have the Firewall Proxy Arp for it.

Debugging the Connect Control Module

The Connect Control Module is one of the "Load Balancing Components" described on page 107. It resides in the kernel of the FireWall Module containing the load balancing algorithm.

The Connect Control Module uses several kernel tables

To debug connect control problems you will almost always need to examine one of the following tables

- Check_alive – this table exists to see if the physical servers are alive. The `in.pingd` process reads the table and sends pings to the servers if a time period has passed.
- `Logical_cache_table` – only when persistent mode is enabled. Holds the information relating to which client connects to which server.
- `Logical_request` – any new connection going through the connect control module is written in that table
- `Logical_server_table` – holds a list of the logical servers.
- `Logical_server_list_table` – if NAT is involved

These tables are described in detail in "Load balancing tables," page 164 of "Appendix A: State Tables for VPN-1/FireWall-1 4.0

Check_alive table

Load balancing takes place between a group of servers. A server will only take part in the load balancing if it is alive. If a server is no longer considered as a valid server the VPN/FireWall module will not redirect packets to that server (it may be down or overloaded for example). The `Check_Alive` table is used to determine whether the servers in the group are alive

The `In.pingd` send Pings to the servers at regular intervals, and a computation based on the values in the table determines whether or not the server is alive.

Check_Alive table

1	2	3	4	5	6	7
IP address	Magic (1 or 2) 1= Client Auth. 2= Load balancing	Last ping time – the time when the server was last pinged (in seconds since 1/1/1970)	Time to die – time until connection is no longer referred to that server, if it does not respond (default 60 sec)	Recheck – number of seconds between each 2 consecutive rechecks	Reference count- how many connections were referred to this server	time left/ total time

The following computation is used to decide if the server is up or down. If the result is TRUE, the server has died:

Time Now – [last time host was pinged (value 3)] > Time to Die (value 4) - When to recheck this host (Value 5)

The `pingd` process is defined in the `fwauthd.conf` file in the `conf` directory. If this process is disabled you will not be able to activate load balancing on VPN-1/FireWall-1.

The following solutions from the SecureKnowledge database solve problems that relate to the tables used by the Connect Control module.

Logical Server of type “Other” using the round robin for the Load Balance does not work

Another symptom is that Logical Server of type Other using the round robin for the Load Balance did work for VPN-1/FireWall-1 4.0 SP1

A possible workaround is to choose for the Time Zone a country, which has the same difference from GMT, but has no problem with Daylight Saving information. For example, in Israel, which is in time zone GMT+02:00, the user may choose Helsinki for the Time Zone, since Helsinki and Israel are in the same time zone, and this will solve the problem.
Cause of this problem: Problem will occur only where the Windows NT option 'Automatically adjust clock for daylight savings changes' is grayed out in the Control Panel> Date/Time Properties>Time Zone. This is the case for some of the countries listed in the time Zone list (Australia or Israel, for example).

In these countries, Daylight Savings information is not available to Windows NT, so that Time objects in the VPN-1/FireWall-1 Rule Base may not work correctly.

This results in VPN-1/FireWall-1 updating the "`check_alive`" table with a wrong time. This is a result of a bug in the compiler used to compile VPN-1/FireWall-1

See the SecureKnowledge Solution (ID: 10043.0.732302.2530987) in the Check Point Technical Services site

How to change the load balancing connection time-out

The Time-to-die value in the in the `check_alive` table (value 4) defines the time until connection is no longer referred to a non-responding server. The default value is 60 seconds. It is possible to modify this value in order to increase the amount of time for which a non-responding connection is considered valid.

To do so, edit objects, and under the `:Props` section Add the following line

```
:logical_servers_timeout  (x)
```

where X represents any number between 0 and 65535

See related SecureKnowledge Solution (ID 21.0.1307045.2432924) in the Check Point Technical Services site.

How long does the Persistent Server Mode last?

The Persistent Server Mode allows a specific client to be assigned a specific server for the duration of the Persistent Server timeout, the default being 30 minutes.

The default persistency timeout is 30 minutes and is refreshable (every new connection to the persistent server will reset the timer). It is defined in the `'$FWDIR/lib/table.def'` file on the management module machine as follows:

```
#define LOGICAL_CACHE_TIMEOUT 1800
```

To change the default timeout, change the value 1800 (seconds) to the desired value in seconds and reinstall the policy.

See SecureKnowledge Solution (ID 10022.0.1112954.2441351) in the Check Point Technical Services site.

How to get a connection to switch to the next server immediately after the server failed

Problem Description: When doing Load Balancing in Persistent mode it takes 30 minutes for the connection to switch to the next server after the first server has failed

Add the following to the `$FWDIR/lib/fwui_head.def` file under `'get <src,dst,dport,rule>` from `LOGICAL_CACHE_TABLE` to `sr10`,'

```
get <sr10, 2> from check_alive to sr6, \
( 3602 - (((sr6 - 2) - tod) %% 3600 ) <= sr7 or \
(delete <src,dst,dport,rule> from LOGICAL_CACHE_TABLE)), \
```

Install the policy.

The switch to the next server will occur after about 30-60 seconds (the `logical_servers_timeout` in the `objects.C` file will affect the switch time)

See SecureKnowledge Solution (ID 10043.0.6634086.2622727) in the Check Point Technical Services site.

Load Balancing does not work properly when using Persistent Server Mode

The Persistent Server Mode allows a specific client to be assigned a specific server for the duration of the Persistent Server timeout, the default being 30 minutes.

The client identifier is limited to the IP address only. Thus, if you have 5 hide NAT clients with the same valid IP address coming in, they will all be assigned to the same persistent mode server.

Cause of this problem: There is no way to distinguish between different clients if they are coming from the same IP, for example an HTTP proxy

See SecureKnowledge Solution (ID 10022.0.1112971.2441351) in the Check Point Technical Services site.

How to synchronize the logical_cache table

In a synchronized environment, you may also want to synchronize the cache table, which is not synchronized by default.

To do so,

1. Edit the `table.def` file and in the cache table definition add the attribute ‘`Sync’`as in the following example

```
LOGICAL_CACHE_TABLE = dynamic refresh sync expires
LOGICAL_CACHE_TIMEOUT limit LOGICAL_CACHE_SIZE;
```

2. Save the file and Install the policy.

How to increase the size of the logical cache

The `logical_cache` is limited to `LOGICAL_CACHE_SIZE` which is set by default to 1000 entries.

To increase it, edit the `table.def` and modify the `LOGICAL_CACHE_SIZE` parameter. For example:

```
#define LOGICAL_CACHE_SIZE 2000
```

Debugging the Load Balancing daemon lhttpd

The Load Balancing daemon `lhttpd` is one of the “Load Balancing Components” described on page 107. Load Balancing daemon (`lhttpd`) is the user mode process that handles HTTP requests, when the load balancing method is set to HTTP. `lhttpd` listens for and redirects HTTP requests coming for load balancing.

The process is defined in the `fwauthd.conf` file

```
10081 in.lhttpd  wait 0
```

You can debug this process by adding an environment variable:

```
Set FWBHTTPD_DEBUG 1
```

Debugging the Server-Load Load balancing algorithm

The Load Balancing algorithm is one of the “Load Balancing Components” described on page 107. There are five available load balancing algorithms: Server Load, Round Trip, Round Robin, Random, and Domain (in the Domain algorithm (for HTTP only), VPN-1/FireWall-1 chooses the physical server “closest” to the client, based on domain names).

How the Server Load algorithm works

In the Server Load load balancing algorithm, VPN-1/FireWall-1 determines the load of each physical server. There must be a load-measuring agent on each physical server. The Load Balancing service on VPN-1/FireWall-1 does not trigger the load agents at each incoming connection request. The load agent is triggered every number of incoming requests, then the result is incremented by one up to a limit, then a new measurement is performed.

About the Load measuring agent

The parameter that affects the load measuring agent

The `lbalance_period_wakeup_sec (30)` parameter affects the load agent. It is set to 30 seconds by default.

How often does VPN-1/FireWall-1 perform server load measurement?

Every "`lbalance_period_wakeup_sec`" seconds the VPN-1/FireWall-1 daemon (`fwd`) wakes up and checks whether the kernel used the load values it produced.

`fwd` does this by looking in table called "`logical_server_table`" for the key "`0xffffffff`", at the second value after the ";". A 0 (zero) value means that the kernel did use the load values.

- If this value is other than 0 a new load measure is taken.

- If this value is 0, a check is made that "`period_until_measure`" has elapsed since the last time a measurement was taken. "`period_until_measure`" is a variable that specifies the number of "`lbalance_period_wakeup_sec`" periods to wait until a new measurement is taken.

This value is increased by 1 each time a new measurement is taken and the load values were not used, until the maximum of 1200 is reached.

Note about the load balancing agent

Unix

The load agent service must be added to the `inetd.conf` file (see product documentation)

The program retrieves the load average value and converts it to a number between 0 to 231.

NT

The load agent service must be added through the Services dialog box.

The program retrieves the privileged time percentage, and re-scales it to the 0-231 range.

Chapter 10: Troubleshooting SNMP

In This Chapter:

Introduction **115**

How to configure HP Open View to work with FireWall-1 4.0 ..... **115**

Resolving Common SNMP Problems **115**

What to check first 115
100% CPU usage when trying to poll information from the FireWall-1 snmpd 116
Unable to run $FWDIR/bin/snmpd -p 161 116

More Information **116**

Troubleshooting SNMP

Introduction

With the increase in the size of the computer network in an organization, it becomes increasingly important centrally manage the variety of network devices. The Simple Network Management Protocol (SNMP) enables a standard way of managing TCP/IP networks. SNMP uses a “Management Information Base” (MIB), which is a tree structure of variables. Every vendor can add appropriate variables to the existing standard ones.

Agents (daemons) are installed on every network device that uses SNMP. Agents are responsible for communication with the management station(s). Thus, a management station has to be defined, so that the agent will know where to send SNMP traps and answers. There are three types of SNMP connections:

- GET – A command used by the management station to query (get MIB variable values) the network element.
- SET - A command to set a MIB variable value at the network element.
- TRAP – When a network element changes its status, it sends a trap (message) to the management station.

For every SNMP command, a community string has to be specified. A community string is a text string that is used as an authentication word. The VPN-1/FireWall-1 default string is “public” for GET commands, and “private” for SET commands.

To learn more about the protocol, read Rfc1157.

In VPN-1/FireWall-1, SNMP is used on Network Objects definitions (the “SNMP fetch” button).

How to configure HP Open View to work with FireWall-1 4.0

Be aware that only the following versions of HP Open View are supported with FireWall-1 4.0:

- HP Open View for HPUX - versions 5.0 and below
- HP Open View for Solaris - versions 6.0 and below

See the configuration document for FireWall-1 4.0: “Installation/Update Procedure for HP Open View and FireWall-1 Interoperability” (ID 55.0.4232364.2607295) in the Check Point Technical Services SecureKnowledge site (29 pages).

Resolving Common SNMP Problems

This section lists some common problems and solution from the Check Point Technical Services SecureKnowledge knowledge base.

What to check first

1. First, check that the SNMP daemon is running. On the NT platform, check that the local SNMP service is used, and if it doesn’t exist, add it by right-clicking on the Network Neighborhood icon and choosing Properties. Then go to the Services tab and add the SNMP service. On Unix platforms use the VPN-1/FireWall-1 `snmpd` (the SNMP daemon, started automatically when the FireWall is started), which is located at `$FWDIR/bin` directory. If the OS SNMP daemon is already started then the FireWall-1 daemon is started at port 260, while the standard port (that is occupied by the other daemon) is 161. If the SNMP daemon doesn’t work, execute the command `snmpd` at `$FWDIR/bin`.
2. In FireWall-1 4.0, the FireWall-1 `snmpd` gets all the SNMP connections and sends them to the OS `snmpd` (if exists) unless they request FireWall-1 information.

3. Make sure that the community strings are correctly defined when trying to establish an SNMP connection. On Unix platforms, the community strings are defined by `$FWDIR/conf/snmp.C` . Network object community strings are defined in the Network Objects window.
4. Use snoop to check SNMP connections.

100% CPU usage when trying to poll information from the FireWall-1 snmpd

One of the most common problems with SNMP is on Solaris 2.6 once you try to poll information about the FireWall tree using the snmpwalk command or a Network management tool that uses the snmpwalk command.

On the management station you get an error message: “snmpwalk: No response arrived before timeout” and on the Agent station the FireWall-1 snmpd used almost 100% of CPU resources.

This problem occurs because of the way SNMPD was run on the machine. On Solaris 2.6 the native SNMPD must run together with the FireWall-1 smpd, otherwise any attempt to poll information fails and causes the system to reach almost of 100% CPU load.

The solution is as follows:

1. Kill both the snmp daemons
2. Run both the native snmpd and the Firewall snmpd together:
   (1) Run **`/usr/lib/snmp/snmpdx`**
   (2) Run **`/usr/lib/dmi/snmpXdmid -s <hostname> -c /etc/snmp/conf`**
   (3) Run **`$FWDIR/bin/snmpd`**

See the SecureKnowledge Solution (ID 10043.0.4616466.2575219) in the Check Point Technical Services site.

Unable to run $FWDIR/bin/snmpd -p 161

Other symptoms are: The `-p` option in `$FWDIR/bin/snmpd -p 161` is not supported, and On HP-UX, AIX and Windows NT, the SNMP daemon binds only to port 260 although port 161 is free

The cause is that the SNMP mechanism was designed to work on HP, AIX and Windows NT with the local SNMP as a proxy. It will always leave port 161 free for the local SNMP daemon. Therefore both daemons should run and queries should be sent to port 260 only.

Upgrade to FireWall-1 4.0 SP6 or FireWall-1 4.1 SP1 that don't include the -p option for snmpd

See the SecureKnowledge Solution (ID 10022.0.1872144.2482146) in the Check Point Technical Services site.

More Information

For more information on SNMP and FireWall-1, see the chapter on SNMP and Network Management Tools in

- FireWall-1 Architecture and Administration User Guide version 4.0, chapter 9.
- VPN-1/FireWall-1 Administration Guides for version 4.1 and Check Point 2000, chapter 18.-

Chapter 11: Troubleshooting Licensing

In This Chapter:

Check Point Licensing Policy 118

VPN-1/FireWall-1 Licensing 118
Licensing Example 1: Single VPN/-1FireWall-1 Gateway 118
Licensing Example 2: Multiple VPN-1/FireWall-1 Gateways 119
Licensing Example 3: intermediate proxy behind the VPN-1/FireWall-1 Gateway 119
Licensing Example 4: Two VPN-1/ FireWall-1 gateways protecting a common internal network 120
Bank Certificate Key (BCK) 120

Product Features Lists 121

Firewall-1 4.0 Features 121
Embedded FireWalls and Third-Party Product Features 121
How embedded Licenses work 121
Remote License Keywords 122

Resolving Common Licensing Problems 122

What happens to the License during an upgrade? 122
When do you need a new License? 122
Which IP should be in the license of a VPN/FireWall module with several interfaces? 122
How to Verify Licenses 122
Licensing synchronized VPN/FireWall modules 123
Licensing non IP hosts 123
The structure of the license as maintained on the system 123
License installation 124
Additional Notes 124
Error: "Failed to add license" when trying to add license via the GUI or "fw putlic" command 125
Error: "No license for <feature>" when trying to do some action 125
Error: "No license for fwm" when trying to open a GUI client. 125
Error: "No license for encryption", even though no encryption is used 125
Error: "only ### internal hosts allowed" 126

Troubleshooting Licensing

For the latest information about operational aspects of Check Point product licensing, see the Check Point License center http://license.checkpoint.com/

Check Point Licensing Policy

VPN-1/FireWall-1 Licensing

Licensing for Check Point VPN-1/FireWall-1 is based on the total number of internal nodes protected. For licensing purposes, a node is any IP address protected by any VPN-1/FireWall-1 interface, excluding the external interface. Protected nodes include all network devices with IP addresses, such as workstations, routers, hubs, printers, etc.

FireWall-1 and VPN-1 gateways track the cumulative number of nodes (IP addresses) on all internal interfaces beginning from initial installation. There is no expiration of IP addresses from this count. A multi-user workstation is counted as a single node. For a multi-homed workstation, the number of nodes is equal to the number of workstation interfaces.

When the FireWall-1 or VPN-1 gateway encounters an IP address that exceeds the license limit, messages will be sent to the console of the VPN-1/FireWall-1 module, and the VPN-1/FireWall-1 administrator will be alerted via email that the license has been violated and should be upgraded immediately.

Licensing based on the number of protected nodes is the most straightforward approach and ensures that all internal users/hosts have secure Internet connectivity. There is never a concern about exceeding a vendor-imposed limit on the number of concurrent sessions.

Licensing Example 1: Single VPN/-1FireWall-1 Gateway

The figure below shows a simple network configuration with VPN-1/FireWall-1 providing Internet security.

For this network, the organization would require a FireWall-1 or VPN-1 product license that supports “n” nodes.

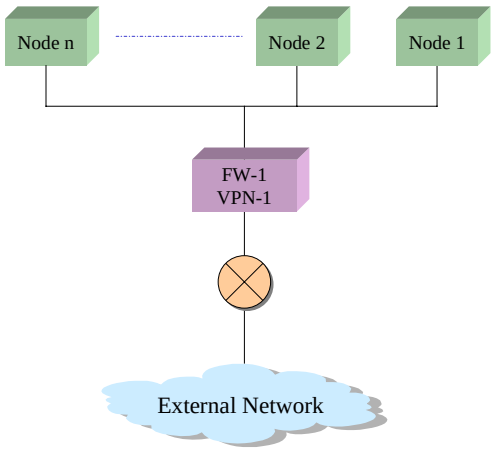


Figure 1. Single VPN-1/FireWall-1 Gateway Licensing requirements

Licensing Example 2: Multiple VPN-1/FireWall-1 Gateways

The configuration below shows a network with two FireWall-1 installations: one providing Internet security, and a second delivering intranet security.

VPN-1/FireWall-1 licensing is based on the total number of protected nodes in the organization. This total includes all nodes connected to a trusted (internal) network either directly, or indirectly via nested subnets linked by routers, FireWalled gateways, etc. For the network shown, the intranet FireWall-1 gateway requires a license that will support “N” nodes. The Internet FireWall-1 gateway requires a license that will protect the total number of internal nodes: “N+n+1” nodes. The one additional node accounts for the Intranet VPN/FireWall machine.

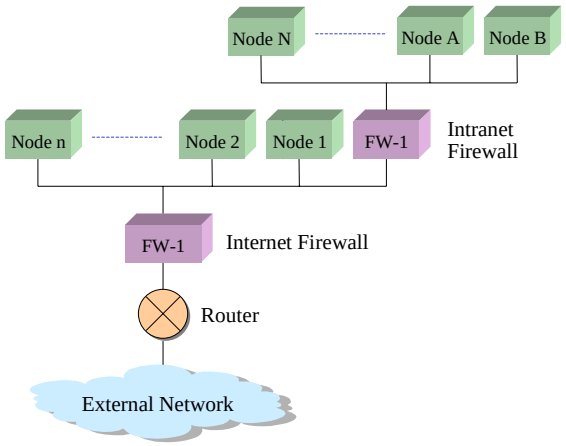


Figure 2. Multiple VPN-1/FireWall-1 Gateway Licensing requirements

Licensing Example 3: intermediate proxy behind the VPN-1/FireWall-1 Gateway

The diagram below shows a network that includes a proxy performing network address translation for the internal nodes.

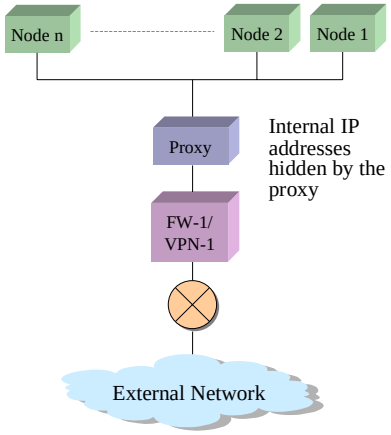


Figure 3. Licencing requirements with intermediate proxy behind the VPN-1/FireWall-1 Gateway

FireWall-1 and VPN-1 licenses are based on the total number of protected nodes. This requirement does not change when using any intermediate proxy or device capable of IP address translation.

For the network shown in the diagram above, the VPN-1/FireWall-1 license must support all "n+1" internal nodes. The one additional node accounts for the Proxy.

Licensing Example 4: Two VPN-1/ FireWall-1 gateways protecting a common internal network

The diagram below shows two VPN-1/ FireWall-1 gateways protecting a common internal network.

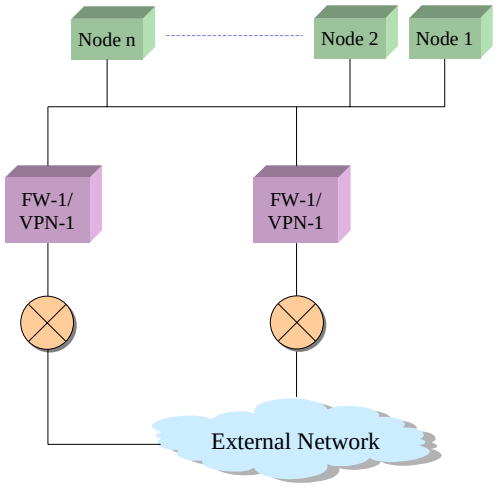


Figure 4. Licencing requirements with multiple VPN-1/ FireWall-1 gateways protecting a common internal network

Each VPN-1/FireWall-1 gateway requires a license that will support all “n” internal nodes. Because each VPN-1/FireWall-1 gateway is protecting all internal nodes, each must be licensed accordingly.

Bank Certificate Key (BCK)

Check Point provides direct partners (partners who place orders directly with Check Point) with a Bank Certificate Key (BCK), which is used to generate a bank of licenses from the on-line licensing center. Each license is tied to a specific IP Address / Host ID Each license is for a period of 30 days. The number of licenses the BCK will generate depends on the volume of your activity and should be sufficient for a period of one quarter.

A direct partner can use the BCK to generate licenses for resellers and end users as well. The BCK should be used in cases of emergency. It is not intended for evaluation purposes (the Certificate Key on the CD should be used for this purpose), nor for in house security and demo centers (for this you can purchase a permanent license at a substantial discount).

The BCK is not intended to be given to resellers or end users to generate their own licenses, but rather the direct partners should do it for them and provide them with the license.

Once a direct partner has generated most of these licenses, they should request a new Bank Certificate Key by submitting a request by email to sales@checkpoint.com. This request must include the following information:

1. The BCK
2. Type of BCK (VPN type)

3. Number of requested licenses per BCK
4. Email address for PO confirmation (The BCK and the number of licenses that it can generate will be sent as a PO confirmation).

Product Features Lists

Firewall-1 4.0 Features

For a complete list of VPN-1/FireWall-1 4.0 features, see the SecureKnowledge Solution (ID: 36.0.285147.2477204) in the Check Point Technical Services site

Embedded FireWalls and Third-Party Product Features

How embedded Licenses work

Every embedded module defined in `objects.C` must have a license installed on the management station. The license must fit both the FireWall-1 version and the number of hosts protected by the embedded module. The number of protected hosts is specified in the Setup tab in the embedded module popup.

In addition, there must also be a '`remote`' license for each embedded module (again – installed on the management station). For example, if three embedded modules have been defined, there must be three `remote` modules (e.g. `remote1 + remote2`).

Table 1: Embedded License Keywords

Keyword:	Supported in VPN-1/FireWall-1 Version:	Meaning:

`embed_40_25`
`embed_40_50`
`embed_40_100`
`embed_40_250`
`embed_40_500`
	4.0 SP-5 and higher	Specify the number of IP addresses on a network protected by one embedded system: 25, 50, 100, 250, or 500

`embed_40_ul`	4.0 SP-5 and higher	For an unlimited number of nodes protected by one embedded system

`embed25`
`embed50`
`embed100`
`ebmed250`
`embed500`
	3.0 and 4.0	Specify the number of IP addresses on a network protected by one embedded system: 25, 50, 100, 250, or 500

`Embedul`	3.0 and 4.0	For an unlimited number of nodes protected by one embedded system

Remote License Keywords

Remote licenses are for remote policy installation on embedded and non-embedded VPN/FireWall modules

Table 2: Remote License Keywords

Keyword:	Supported in VPN-1/FireWall-1 Version:	Meaning:

`remote1`
`renmote2`
`remote4`
	4.0 SP5 and higher	The numbers at the end of the keywords specify the number of licenses (e.g. `remote2` specifies two licenses for remote installation).

`remote`	3.0 and 4.0	Specifies an unlimited number of licenses for remote installations
`lcontrol`		A management license required for the operation of the management station
`control`		Equivalent to `lcontrol + remote`. It is a license a management station and policy installation on an unlimited number of remote modules (embedded and not embedded)

Resolving Common Licensing Problems

This section lists some common problems and solution. Most can be found on the Check Point Technical Services SecureKnowledge knowledge base

What happens to the License during an upgrade?

When you upgrade FireWall–1 to a new version, you can continue to use the old licenses. The licenses are different in every new major version, so that you must obtain a new license when upgrading from version 4.0 to 4.1, for example.

Resellers are informed if there is a change in the licensing in a new version.

When do you need a new License?

If the license is tied to the `hostid`, it will need to be changed whenever the computer is changed. If the license is related to an IP address that is no longer the machine IP address, the customer will receive a new license key free of charge, provided they guarantee they won't use the old one again.

Which IP should be in the license of a VPN/FireWall module with several interfaces?

If a VPN/FireWall module has more than one interface, the Check Point license can be based on any of them. However, it is recommended that the license be issued for the IP that is associated with the system's name in the name resolution databases.

`encryption` licenses (and any other license that includes the `encryption` feature) need to have the IP address of the interface on which encryption takes place (i.e., the external one).

This is recommended for any other license feature as well.

How to Verify Licenses

To verify licenses, issue the command **`fw printlic`**. The output should be similar to the following:

```
Type      Expiration Ver  Features
Eval      15Jul96    4.x  pfm control routers
807dafa7  Never      4.x  pfm control routers encryption [Invalid]
807dafa8  Never      4.x  pfm control routers encryption
807dafa7  Never      3.x  pfm control routers encryption
807dafa7  Never      4.x  pfm control routers encryption
```

The FireWall in question contains four licenses. The first is an evaluation license, which is valid for all computers, but only until July 15th, 1996. The second is an invalid license, probably because of typos in the license string. The third is a permanent license for hostid `807dafa8`, which is perfectly valid but irrelevant because the hostid is `807dafa7`. The fourth license is also valid, but allows us to run FireWall-1 v. 3.x only, and not VPN-1/FireWall-1 4.x. Only the latter license (which never expires, is valid, and is for the correct hostid, and has the correct version), is actually used.

When verifying licenses on the firewall, it is important to remember that even if a license is displayed as valid, it may still be irrelevant because of either date or hostid. If several relevant licenses are installed, their features are “OR”ed together.

To check whether a certain license feature exists in your license (whether explicitly, or included in a combined license feature), use the command **`fw checklic`** `<feature>`.

Both the **`fw printlic`** and the **`fw checklic`** commands allow you to use a "`-k`" switch in order to perform the check upon the license embedded in the kernel module rather than upon the one in `$FWDIR/conf/fw.LICENSE` (`%systemroot%\fw\conf\fw.LICENSE` on NT)

See the SecureKnowledge Solution (Solution ID: 3.0.698740.2304823) in the Check Point Technical Services site

Licensing synchronized VPN/FireWall modules

Two synchronized VPN/FireWall modules need to have two '`pfm`' or `pfi` licenses. If these modules are limited modules (25, 50, 100, or 250 hosts), you also need the `highav` feature in the license. It is recommended to also have a management station with the `control` feature, which is able to control both modules. It can be on the same machine as the two modules, or on a third machine.

Two machines, both with '`stdlight25`' licenses (i.e. two FIG-xxx products), may also be synchronized, though this is far less convenient. A connect control module, however, is not needed for this feature.

Licensing non IP hosts

You have to buy a license based on the number of internal network computers that run TCP/IP only, rather than including the non-TCP/IP ones.

The structure of the license as maintained on the system

The internal structure of the license maintained in the system cannot be seen. It is described here for a better understanding of the way license is enforced.

Host id or ip address	Expiration	Features	Signature

There can be up to 32 licenses on one machine.

The signature is built by an algorithm that uses the “`host id`” or “`ip address`”, ”`expiration`” and “`features`” values. The putlic command installs the license. The generated structure is the following:

Host id/ip address	K1-k2-k3 (license string)	The features

The license string components are as follows:

K1: holds the expiration date of the license.
K2, K3: holds the signature of the unique license.

The signature is checked according to the 3 fields.

License installation

Table 3: Location of License file for VPN-1/FireWall-1 versions 4.0 and 4.1

Product	Location of License file
VPN-1/FireWall-1 4.0 on NT	Registry path: HKEY_LOCAL_MACHINE/STSTEM/CurrentControlSet/Services/FW1/Parameters/License (There is no need for specific installation of the license on the kernel.)
VPN-1/FireWall-1 4.0 on UNIX	file: `$FWDIR/conf/fw.license` (Used by `fw` and `fwui` applications)
VPN-1/FireWall-1 4.1 on NT	Registry path: HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\License (This path should be created by the installation.)
VPN-1/FireWall-1 4.1 on UNIX	file: $FWDIR/conf/cp.license.

The license installation procedure depends on the Operating System, as follows:

Table 4: License installation procedure

OS	License file	Installation's procedure
Solaris	fwmod.5.x.o	fw putlic –K
SunOS4	fwmod.4.xo	
Solaris x86	fwmod.5.x.o	
HPUX 10 HPUX 9	fwmod.hpux10.o/ fwmod.hpux9.o	When fwstart runs the putlic command is launched automatically
AIX	fwmod.4.x.o	

Additional Notes

1. VPN-1/FireWall-1 4.0 On UNIX

To install the license in the kernel use the command `putlic –k`.

The flag –k is used to force the installation on the kernel.

On Unix the kernel license is put in the kernel driver found under the `$FWDIR/modules/` directory.

The command `fw putlic –K` (with uppercase K) forces license installation both in the license file and the kernel.

The command "`putlic –K`" must be used when new modules are installed. This is relevant only for the Solaris / SunOS / Solaris x86 Operating Systems.

2. **The cp.macro file**

There is a new file on VPN-1/FireWall-1 4.1 on NT and UNIX called `$FWDIR/conf/cp.macro`. It contains mapping between product SKUs and license features and grouping of features.

Error: "Failed to add license" when trying to add license via the GUI or "fw putlic" command

The cause for these messages could be one of the following:

1. The license may have been mistyped
2. There are occasionally problems when installing licenses from the GUI

Check your license, and the "`fw putlic`" command you performed. Note that 'I', 'l' and '1' are different characters, and so are '0', 'O' and 'o'.

Also make sure you did not omit any of the features in the feature list.

Try installing the license using the command line ("`fw putlic`"), which is more reliable.

If the problem is still not solved, contact the Check Point licensing center and ask them to issue a new license. Inform them that previous license is faulty.

Error: "No license for <feature>" when trying to do some action

Usually, the error is due to the fact that the license is issued for the wrong host-id/IP-address

Look at the outputs of: `fw printlic` , `fw printlic -k`, `fw checklic <feature>` and `fw checklic -k feature`.

Check these outputs to see if you have this feature both in the license file and in the kernel. If you do not have the appropriate license, contact your reseller (or license@checkpoint.com, if you are entitled to direct support) to obtain one.

In case of an IP address-based license: the IP address should be the one to which the host name is resolved. If this is an encryption license, it should have the IP address of the interface on which encryption takes place. If the feature exists in the license file, but does not exist in the kernel, issue `fw putlic -k`.

If all the license features seem to exist everywhere, and these messages still appear, run the action that you were trying to perform in debug mode (e.g. `fwm –d`, `fwd -d`, `fw load -d`) and send the debug output to Check Point Technical Support. This will let them check why FireWall-1 thinks the license is invalid when performing this action

Error: "No license for fwm" when trying to open a GUI client.

In case of a motif GUI, you should obtain a `motif` license. You can get it for free on http://license.checkpoint.com by providing your certificate key. You need to get this license for the Management's IP address.

In case this is a Windows GUI, the feature needed is `control`. Check if you have that feature, as specified in Error: "No license for <feature>" when trying to do some action

Error: "No license for encryption", even though no encryption is used

If you are using distributed management (the management station is not on the same machine as the VPN/FireWall module), you should edit the `lib/control.map` file on both sides, and replace every occurrence of `fwa1` with `skey` .

You will still get some messages at startup (that is, whenever `fwd` is started - on boot-time or `fwstart`), but these are just warnings that can be ignored.

Error: "only ### internal hosts allowed"

This warning message can be ignored if it

- Appears only when `fwd` is started
- Is not followed by a list of IP addresses
- Causes no problem in the operation of VPN-1/FireWall-1 operation, and
- Specifies the true number of hosts allowed

If you get a list of so-called 'internal' IP addresses detected, check if they are all internal, or whether some of them are external. If they are all internal, upgrade to a bigger product. If some are external, make sure your `conf/external.if` file includes the name of your external interface, as found in the output of "`ifconfig -a`" (UNIX) or '`ipconfig /all`' (NT).

If the list of IP addresses is not available, you can alternatively get the `database/fwd.h` file to a UNIX machine, and issue the `od -t u1 fwd.h` command. You will get a list of numbers each between 0 and 255. Each 4 consecutive numbers are an IP address. Alternatively, you can issue the `fw lichosts` command to get a log of the internal hosts detected (note that this command may take some time to complete).

After the reason to the problem is found, you need to delete the `database/fwd.h` and `database/fwd.hosts` file and restart the `fwd`. If the reason to the problem no longer exists (e.g. the network previously had too many hosts, but now it no longer does) this would solve the problem.

On HP machines, the error message "only 25 internal hosts allowed" which appears after a boot can be ignored. It is printed before the license is loaded into the kernel, and therefore it is not yet found in that stage.

For more information about exceeding the number of hosts for a license, see the SecureKnowledge Solution (ID: 3.0.188485.2208447) in the Check Point Technical Services site.

Chapter 12: What To Send Technical Support

In This Chapter

Introduction **128**

Rule Base **128**

Network Address translation **128**

Anti Spoofing **128**

INSPECT **129**

GUI **129**

LOG **129**

High Availability **130**

Security Servers **130**

Authentication 130
Resources and CVP servers 130

LDAP **131**

Routers and Embedded Systems (OEM) **131**

BAY Router 131
Bay CES 131
Xylan 131

Open Security Extension (OSE) **132**

Crashes **132**

CORE 132
Dr. Watson 132

What To Send Technical Support

Introduction

In order to solve your problem, your technical support representative will need all relevant information about the problem and its environment. For each type of problem, the Support representative will ask for specific records and files.

Sending this information as soon as the Support Call is opened will make the handling of the ticket more efficient and will ensure that the problem is resolved as quickly as possible

This chapter lists the information that Check Point Support will ask you to gather for each type of problem. It may also be of use when doing your own troubleshooting.

See Chapter 2: Troubleshooting Tools“Chapter 2: Troubleshooting Tools,” page 5 for more information on the `fwinfo, fw monitor` and the `fw ctl debug` commands.

Rule Base

1. `fwinfo` file.
2. Relevant `fw monitor` file.
3. Relevant log records.

Send the files to support@ts.checkpoint.com

Network Address translation

Gather the following information:

1. `fwinfo` file.
2. A sketch of the network configuration.
3. `fw monitor` file on both FireWall-1 Interfaces (or, preferably, the appropriate `fw monitor`, which is better in this case).
4. Issue the command

```
fw ctl debug –buf
fw ctl debug xlate
fw ctl kdebug -f > /tmp/kdebug.out
```

   In case of FTP or TELNET, you can add the option `xltrc` after the `xlate` option.

5. After the problem occurs, stop this command with `^C`, and run `fw ctl debug 0`.

Send the files to support@ts.checkpoint.com

Anti Spoofing

1. `fwinfo` file
2. Network Diagram

Send the files to support@ts.checkpoint.com

INSPECT

If a specific Service is suspected as being part of the problem, gather the following information

1. How does the service work?
2. On which protocol does the service work?
3. On which ports does the service work?
4. `fw monitor` files are important to understand the protocol.
5. If you want to debug the Inspect code, you can add debug statements in the code, such as the following:
   `Debug dport`

   Or, if you want to print out more than one value:
   `Debug <0x369, sr4, [68:5,b]>`

   Then, to see the debug output run
   `fw ctl debug` and `fw ctl kdebug -f`.

Send the files to support@ts.checkpoint.com

GUI

1. Make sure that the edition of the GUI Client is compatible with the Management station.
2. `fwinfo` file.
3. Error messages from the log and from the screen.
4. Issue the command `fwm –d > file.`

Send the files to support@ts.checkpoint.com.

LOG

Gather the following information:

1. `fwinfo` file.
2. Log files.
3. If the problem is related to the Log Viewer, issue the command `fw logexport` to see if all the columns are full.
4. If the log records are not written to the log file (`fw log` and `fw logexport` show no new records), you may want to run `fw d –d –D`, which includes special debugging option for `FW1_LOG` connections.

Send the files to support@ts.checkpoint.com.

High Availability

1. `fw monitor` file that is relevant for the problem.
2. `fwinfo` file from management and both modules.
3. `sync.conf` file on both sides.
4. Network topology.
5. Issue the command
   `fw tab –u –t  connections > file`
   on both VPN-1/FireWall-1 machines at the same time (connections may be replaced by any other table that should be synchronized but isn't).

Send the files to support@ts.checkpoint.com.

Security Servers

Authentication

Gather the following information:

1. `fwinfo` file.
2. Error messages from the log and from the screen.
3. `fw monitor` file that is relevant for the problem.
4. Send the `log/ahttpd.log` file to support@ts.checkpoint.com.
5. If the problem is related to SMTP, ask for the spool directory and run the mail dequeuer and the `asmtpd` in debug mode.

Send the files to support@ts.checkpoint.com.

Resources and CVP servers

Gather the following information:

1. `fw monitor` on port 18181.
2. `fwopsec.conf` file.
3. `cvp.conf` file on the CVP side.
4. Set the environment variable `OPSEC_DEBUG_LEVEL` to 3, and restart `fwd`. Send the output received in `fwd.log` to support@ts.checkpoint.com.

LDAP

1. `fwinfo`
2. LDAP log files
3. `fw.log`
4. `fw monitor` :
   between the client and the FireWall
   Between the FireWall and the LDAP
5. Problem description and LDAP version

Send the files to support@ts.checkpoint.com.

Routers and Embedded Systems (OEM)

BAY Router

1. Router's `config` file.
2. Output of `stamp` command.
3. Router model (BLN, ASN, ARN).
4. `Control.map` and `clients` files.
5. `fwinfo` of the management.

Send the files to support@ts.checkpoint.com.

Bay CES

1. CES image version.
2. `fwinfo` of the management.
3. `fwinfo` of the module (CES).

Send the files to support@ts.checkpoint.com.

Xylan

1. Image version (if it's newer than 3.1.6 then, send the image files).
2. `Control.map` and `clients` files.
3. `fwinfo` of the management.

Send the files to support@ts.checkpoint.com.

Open Security Extension (OSE)

Bay

1. Router's `config` file.
2. Output of "`stamp`" command.
3. Router's model (BLN, ASN, ARN).
4. `fwinfo` of the management (if it's VPN-1/FireWall-1 with an OSE feature). Or the `conf` directory

Send the files to support@ts.checkpoint.com.

Cisco

1. A copy of the router configuration
2. Cisco software version.
3. `fwinfo` of the management (if it's VPN-1/FireWall-1 with an OSE feature). Or the `conf` directory.

Send the files to support@ts.checkpoint.com.

Crashes

CORE

Gather the following information:

1. Core File (called `core` for a process core. In case of a kernel panic, send the `vmcore.*` and `vmunix.*` files instead).
2. f`winfo` taken from the system while in the status that caused the core.
3. Full description of the problem (when it occurred, how often etc.).

Send the files to support@ts.checkpoint.com.

Dr. Watson

Gather the following information:

1. Dr. Watson file (`drwtsn32.log`).
2. f`winfo` taken from the system while in the status that cause the Dr. Watson.
3. Full description of the problem.
4. u`ser.dmp` file (`system.dmp` in case of a blue screen crash).

Send the files to support@ts.checkpoint.com.

Chapter 13: Check Point Support Information

The latest version of this chapter can be found on the Check Point Technical Services Premium Support site at http://www.checkpoint.com/support/technical/general_info.html

In This Chapter

Mission Statement **134**

Check Point Worldwide Technical Services General Process **134**

Availability of Check Point Worldwide Technical Services **134**

Contacting Check Point Worldwide Technical Services by Telephone **134**

Contacting Check Point Worldwide Technical Services by E-mail **136**

Problem Severity Definitions **137**

Software Versions Supported **137**

Escalation Procedure **137**

Check Point Support Information

Mission Statement

Check Point Worldwide Technical Services is committed to building strategic relationships with Check Point customers by providing consistent, dependable, high quality, measurable services which effectively utilize Check Point Software Technologies Ltd. products to meet network connectivity and security objectives.

Check Point Worldwide Technical Services General Process

Check Point Worldwide Technical Services utilizes a multi-tier support model for processing issue reports. When initial contact with Worldwide Technical Services is made, a Support Center Team Member will validate all contract information and gather details relevant to the question or issue. A unique trouble ticket number will be assigned and delivered to the designated contact, either verbally, or via electronic mail. This trouble ticket number will be used to track any given issue from initial contact to final resolution.

If appropriate, an issue will be reproduced in our Test Lab. Additional testing and problem duplication may take place in a network laboratory environment. Further investigation, including additional troubleshooting or debugging activity may be required. Based on the results of the Test Lab investigation, an issue may be brought to resolution, or, if an anomaly is identified, escalated to Escalation Management. When an anomaly is identified, or an enhancement request is received, the issue will escalate via Escalation Management to Research & Development [Engineering].

Availability of Check Point Worldwide Technical Services

The Technical Support Call Center operates (subject to conditions beyond our control) seven (7) days a week, twenty-four (24) hours a day, three hundred sixty-five (365) days a year.

Availability of Technical Support is subject to the conditions of the level of individual Support Contracts.

Platinum Support	Direct telephone and e-mail access to technical specialists for problem resolution, bug reporting, documentation clarification and technical guidance, 24 hours a day, 7 days a week.
Gold Plus Support	Direct telephone and e-mail access to technical specialists for problem resolution, bug reporting, documentation clarification and technical guidance, 24 hours a day, 7 days a week.
Gold Support	Direct telephone and e-mail access to technical specialists for problem resolution, bug reporting, documentation clarification and technical guidance, on normal business days, Monday through Friday, during 6:00 am to 6:00 pm local time for the Americas, and Monday through Friday 8:00 am to 8:00 pm local time for the rest of the world.

Contacting Check Point Worldwide Technical Services by Telephone

Dial: 817-606-6600

An Automatic Call Direction System (ACD) will prompt you to select your customer support level.

At this point, you will be directed to a Support Center Team Member. You will be asked for your organization's support number that will be given to you as part of your Support Registration Process. After it is verified that your Support ID is valid, the Support Center Team Member will create a trouble ticket tracking number in the Check Point database. You may be asked to provide or verify some of the following information. If it is not

possible to provide this information, Check Point may be hindered in the ability to bring resolution to an issue in a timely fashion.

1. Complete contact information, (name, title, company name, e-mail address, phone number, pager number, fax number, onsite phone number, time zone) for all parties involved in the issue. If the issue is related in any way to licensing, please provide certificate keys and purchase order numbers for the applicable product.
2. Describe hardware platform(s) involved in this issue, including the amount of memory, disk space, and NIC card types (manufacturer and model).
3. Describe the operating system(s) involved in this issue, including the version number and patch level information. (Include which service pack and Hotfixes for NT, which patches for Solaris, etc.).
4. Provide a detailed description of the problem or issue, including any symptoms noted, any patterns seen (time of day or only certain users affected, etc…) and any specific error messages received.

The Support Center Team Member will then attempt to help resolve the issue. If the issue cannot be resolved via the phone, the issue will be transferred to the Check Point Test Lab. Once it has been determined that the issue cannot be resolved via the phone, you may be asked to submit some additional information which could include the following or other items:

1. Execute the `$FWDIR/bin/fwinfo` command on all FireWall-1 modules and the FireWall-1 management station in question, divert the output to a file, and ATTACH (do not embed), the file to an initial e-mail message.
2. Provide a detailed description of the network topology including, but not limited to: physical network parameters, media and protocols.
3. Location map (topology diagram) of all segment routers and transitional gateways.
4. IP addresses of all router and gateway interfaces.
5. General information about the network, including: approximate number of users, approximate number of simultaneous sessions per user, types of applications in use, etc.
6. An electronic topology diagram is preferred - Visio® or PowerPoint® are good applications to use for this. If this is not feasible, a fax of hand drawn diagrams is an acceptable alternative, provided the IP addresses or Host ID information is legible.
7. Provide a historical description of the problem or issue, from the customer's perspective, detailing chronology and troubleshooting efforts already completed. If FireWall-1 has been upgraded or "backed down" for any reason, please also detail which versions were involved.
8. Provide any miscellaneous, related information. This would include debugging output, packet traces, core dump files, Dr. Watson error logs, FireWall-1 logs, etc.

In the event Check Point is unable to diagnose and, where appropriate, resolve a problem through WTS access, then Check Point agrees to escalate the problem resolution in accordance with the Check Point escalation procedure. In all cases, Check Point will provide the customer a respective trouble ticket tracking number for all calls from the customer.

In the event that Check Point assesses the call to be a non-Check Point defect or failure, Check Point will immediately contact the designated customer contact.

Contacting Check Point Worldwide Technical Services by E-mail

E-mail: support@ts.checkpoint.com

All requests to open a trouble ticket will be routed to the Check Point WTS call-tracking database. A Support Center Team Member will send a response with a unique Trouble Number. The format for the unique Trouble Number will be as follows: ["n" is a numeric digit]

TTnnnnnn: Trouble tickets created by Check Point WTS Call Center.

All electronic mail transactions to and from Check Point WTS must be copied to or sent directly to support@ts.checkpoint.com, and must include the Support ID delimited by pound signs somewhere in the subject line, as illustrated in the following format:

Re: FW-1 will not forward FTP packets on Tuesdays #SUPPORT ID#

With regards to linking new mail to existing trouble tickets - as long as the engineer writes a reply to e-mails from Check Point WTS, the Trouble Ticket Signature should be in the body of the e-mail somewhere. Signatures are sent in all replies coming from Check Point and look something like this:

Do not remove or modify this line: Signature#613132082756#

PLEASE NOTE: If you do not receive an e-mail reply acknowledging receipt of your e-mail request for support within two (2) hours, you should assume that the e-mail link is down, and proceed to make a voice call to Worldwide Technical Services.

In order to expedite the processing and resolution of individual issues, and to maintain and improve Check Point service quality, it is essential that certain information accompany any initial e-mail request.

1. When contact is initiated via electronic mail, the "Subject:" line should include a brief summary of the issue and must include the Support ID delimited by pound signs: Example: "FW-1 v4.0 Service Pack 3 installation question. #SUPPORT ID#"
2. Complete contact information, (name, title, company name, e-mail address, phone number, pager number, fax number, onsite phone number, time zone) for all parties involved in the issue. If the issue is related in any way to licensing, please provide certificate keys and purchase order numbers for the applicable product.
3. Describe the hardware platform(s) involved in this issue, including the amount of memory, disk space, and NIC card types (manufacturer and model).
4. Describe the operating system(s) involved in this issue, including the version number and patch level information. (Include which service pack and Hotfixes for NT, which patches for Solaris, etc.).
5. Provide a detailed description of the problem or issue, including any symptoms noted, any patterns seen (time of day or only certain users affected, etc…) and any specific error messages received.
6. Execute the `$FWDIR/bin/fwinfo` command on all FireWall-1 modules and the FireWall-1 management station in question, divert the output to a file, and ATTACH (do not embed), the file to an initial e-mail message.
7. Provide a historical description of the problem or issue, from the customer's perspective, detailing chronology and troubleshooting efforts already completed. If FireWall-1 has been upgraded or "backed down" for any reason, please also detail which versions were involved.

Check Point understands that due to unusual circumstances, it may not always be feasible to include all of this information in an initial e-mail In order to provide better service, Check Point requests this information as soon as possible, as access to the appropriate data and information facilitates problem resolution. If it is not possible to provide this information, Check Point may be hindered in the ability to bring resolution to an issue in a timely fashion.

Problem Severity Definitions

Severity 1 error	An error that renders product inoperative or causes the product to fail catastrophically; e.g. major system impact, system down. A reported defect in the licensed product which cannot be reasonably circumvented, in which there is an emergency condition that significantly restricts the use of the licensed product to perform necessary business functions. Inability to use the licensed product or a critical impact on operation requiring an immediate solution.
Severity 2 error	An error that substantially degrades the performance of the product or materially restricts business; e.g. moderate system impact, system hanging. This classification is a reported defect in the licensed product which restricts the use of one or more features of the licensed product to perform necessary business functions but does not completely restrict use of the licensed product. Ability to use the licensed product, but an important function is not available and operations are severely impacted.
Severity 3 error	An error that causes only a minor impact on the use of the product; e.g. minor system impact, performance/operational impact. The severity level three defect is a reported defect in the licensed product that restricts the use of one or more features of the licensed product to perform necessary business functions. The defect can be easily circumvented. The error can cause some functional restrictions but it does not have a critical or severe impact on operations.
Severity 4 error	A reported anomaly in the licensed product which does not substantially restrict the use of one or more features of the licensed product to perform necessary business functions. This is a minor problem and is not significant to operation. Anomaly may be easily circumvented or may need to be submitted to Research and Development as a request for enhancement.

Software Versions Supported

Check Point will provide Support to authorized, registered customer with active Support Contracts for the current and the immediately Previous Sequential Major Release of the Check Point Software.

Previous Sequential Major Release is a release of product, which has been replaced, by a subsequent release of the same product.

Notwithstanding anything else, Check Point will Support the previous sequential release only for a period of eighteen (18) months after release of the subsequent release. (That means that Check Point will only Support the older version of the Software for eighteen months after a new version comes out.)

Escalation Procedure

Regardless of the total elapsed time of an outstanding ticket, the point of escalation is initiated at the engineering level, escalated to the Team Lead, and followed by the Support Center Manager(s).

Should an issue require managerial attention, any Technical Services team member will, upon request, connect customer to a manager directly. The formal manager escalation path for all Check Point office locations is as follows:

- Technical Services Team Leader
- Technical Services Manager, Corporate Manager, OEM Manager, Bench Test Manager, Escalations Manager
- Technical Services Director, Escalations Director
- Vice President-World Wide Technical Services

© 2000 Check Point Software Technologies Ltd. All Rights Reserved.

Appendix A: State Tables for VPN-1/FireWall-1 4.0

In This Appendix:

What are State Tables? 141

fw tab 141
Syntax 141
Options 141
Table Attributes 142

The basic structure of a connection in a table entry 142

General tables 143

connections table 143
r_ctype 143
r_cflags 144
old_connections table 145
conn_oneway table 145
estab_table table 145
frag_table table 146
hold_table table 146
pending table 146

SAMP tables 147

sam_blocked_ips table 147
sam_blocked_servs table 148

License enforcement tables 148

host_ip_addrs table 148
forbidden_tab table 148
host_table table 149

Logging tables 149

logged table 149
tracked table 149
trapped table 150
dup_con table 150
domain_cache table 150
arp_table table 150
fwul_table table 150
fwsm_ioctl table 150
synatk_table table 150
fw_route table 151

NAT tables 151

Address Translation Connection tables 151
fwx_forw table 151
fwx_backw table 151
Address Translation “partial connections” tables 152
fwx_anticipate table 152
fwx_anticpate_rev table 152
fwx_alloc table 152
fwx_auth table 153
fwx_frag table 153

VPN tables....153
Encryption tables....153
decryption_pending table....153
encryption_requests table....153
rejected_encryptions table....154
rdp_table table....154
cryptlog_table table....154
SKIP tables....154
skip_connections table....154
skip_key_requests table....155
skip_table table....155
skip_keyid table....155
IKE tables....156
ISAKMP_ESP_table table....156
ISAKMP_AH_table table....156
IPSec tables....156
manual_table table....156
SA_requests table....156
SPI_table table....157
SecuRemote — client side tables....157
enc_timer table....157
userc_topology table....157
userc_session table....158
userc_encapsulating_gateways table....158
userc_request table....159
SecuRemote — server side tables....159
userc_rules table....159
userc_encapsulating_clients table....160
userc_dont_trap table....160
userc_bind table....161
IPSEC_userc_dont_trap_table table....161
userc_request_extended table....162
userc_resolved_gw table....162
userc_DNS_A table....162
userc_DNS_PTR table....162
userc_encrypt_DNS table....162
Security servers and authentication tables....162
auth_services table....162
client_auth table....162
client_was_auth table....163
proxied_conns table....163
autoclntauth_fold table....164
session_auth table....164
session_requests table....165
Load balancing tables....165
check_alive table....165
logical_requests table....165
logical_servers_table table....166
logical_servers_list_table table....166
logical_cache_table table....167

Specific services tables....167

icmp_connections table....167
h323_tracer_table table....167
wf_connections table....168
rtsp_tab table....168
Netshow_tab table....169
Cooltalk_datatab table....169
Sqlnet_port_tab table....169
X11_verify_tab table....169

RPC tables....169

rpc_sessions table....169
rpc_serv_hosts table....169
rpc_serv table....169
pmap_req table....170
pmap_not_responding table....170

DCE/RPC tables....171

dcerpc_maps table....171
dcerpc_binds table....171
dcerpc_portmapper_requests table....171
dcom_objects table....171
dcom_remote_activations table....172
Exchange_notifiers table....172

IIOP tables....172

iiop_port_tab table....172
iiop_requests table....172
iiop_servers table....172

Static tables (lists)....172

cvp_servers_list table....172
firewalled_list table....173
Object Lists tables....173
radius_servers_list table....173
servers_list table....174
tcp_timeouts table....174
tcp_services table....174
udp_services table....174
Time Objects tables....175
ufp_servers_list table....175
table_target_list tables....175

State Tables for VPN-1/FireWall-1 4.0

Note: The information in this appendix is updated to VPN-1/FireWall-1 4.0 SP6. The information for VPN-1/FireWall-1 4.1 and 4.1 SP1 (Check Point 2000) is virtually the same, apart from the addition of new tables in the later versions.

What are State Tables?

State tables are used to keep state information which the FireWall-1 virtual machine (and, in several cases, other components of FireWall-1) need in order to correctly Inspect the packet. The tables are actually the "memory" of the virtual machine in the kernel, and are the key component in Check Point's Stateful Inspection technology.

A discussion of Stateful Inspection can be found in the VPN-1/FireWall-1 Administration Guide (versions 4.1 and Check Point 2000) and in the Architecture and Administration Guide (version 4.0)

The tables are implemented as dynamic hash table in the kernel memory.. All field values are in hexadecimal, apart from the timeout value at the end of the entry (where present).

fw tab

fw tab displays the content of INSPECT tables on the target hosts in various formats.

For each host, the default format displays the host name and a list of all tables with their elements

Syntax

```
fw tab [-all |-conf confile] [-s][-m  number][-u][-t tname][-x tname][-d]
targets
```

Options

parameter	meaning
`-all`	The command is to be executed on all targets specified in the default system configuration file (`$FWDIR/conf/sys.conf`)
`-conf conffile`	The command is to be executed on all targets specified in `conffile`
`-s`	Summary of the number of entries in each table: host name, table name, table ID, and its number of entries
`-m  number`	For each table, display only its first number of entries (default is 16 entries at most)
`-u`	Do not limit the number of entries displayed for each table
`-t tname`	Displays only `tname` table
`-x tname`	Delete all the entries in tname.
`-x`	Delete all entries in all tables
`-d`	Debug mode
`targets`	Run from the management station, for a remote VPN/FireWall module

Table Attributes

A table may have the following attributes:

Attribute	Description
expcall <function>	Call function when an entry is deleted or expires from this table. Can also appear as “free function”.
expires <time>	The amount of time the connection is allowed to stay in the table.
hashsize <size>	In the connections table, the size of the connection table hash. This value should be the power of 2 closest to the size of the table.
implies <table_name>	When an entry goes out from this table it will go out from the specified table.
kbuf <x>	The xth argument in the value section is a pointer to an internal data structure (mostly used in encryption).
keep	Keep the entries after a reinstallation of the policy.
limit <x>	Maximum number of entries that are allowed in the table.
refresh	Reset the expiry timer whenever an entry in the table is accessed.
sync	Synchronize this table if using FireWall-1 Synchronization.

The basic structure of a connection in a table entry

Many tables store entries that represent connections. In those tables, the first five fields follow a common standard. An example of these five fields is shown below along with the meaning of each field..

Other connections in other tables will, in most cases, contain the same five key fields but will store different field values. These first five fields are known as the “key” part of the table entry.

```
<c7cb4764, 0000008a, c7cb47ff, 00000050, 00000006 … >
```

Field	Example value	Description
1	c7cb4764	Source IP address
2	0000008a	Source port
3	c7cb47ff	Destination IP address
4	00000050	Destination port
5	00000006	IP protocol number, as defined in RFC 1700 (11 – UDP, 6 – TCP 1 – ICMP…)

Note: FireWall-1 is able to search on the “key” entries of the table.

General tables

connections table

The connections table contains data on all active connections.

Example

```
attributes: refresh, expires 60, expcall 133279992 4, implies 2, kbuf 1,
hashsize 8192
<c7cb4764, 0000008a, c7cb47ff, 00000000, 00000011; 00000000, 00000002,
00000000; 39/40>
<c7cb4765, 0000008a, c7cb47ff, 00000000, 00000011; 00000000, 00000002,
00000000; 37/40>
```

The connections table uses the following format:

Field	Example value	Description
1.	`c7cb4764`	source IP address
2.	`0000008a`	source port
3.	`c7cb47ff`	destination IP address
4.	`00000000`	destination port
5.	`00000011`	IP protocol
6.	`00000000`	r_ckey. This field is a pointer to the encryption key if the connection is encrypted, otherwise it is NULL
7.	`00000002`	r_ctype. Described below
8.	`00000000`	r_cflags. Described below
9.	`39/40`	time left/total time. There are x of y seconds left until the entry times out and is deleted from the table

r_ctype

The r_ctype field contains eight hexadecimal digits in the form 0000klmn. The last four digits of the value are interpreted using the tables below.

Value of 'n'	Description
1	TCP connection
2	UDP connection
3	Connection is encrypted
4	Reverse connection is encrypted

Value of 'm'	Description
0	Other
8	IPSec connection

Value of 'l'	Description
0	Match by protocol (the most common value)
1	Match by offset (never used)
2	Match by RPC (for RPC connections)
3	Match by getport (for RPC connections)
4	Match by callit (for RPC connections)
5	Match by seq/ack change (for encrypted/NATed connections where the SEQ/ACK numbers may be changed

Digit 'k' is interpreted as four binary digits of the form 0xyz. If a bit in any position is set to 1, the corresponding value in the table below is assumed.

Bit of digit 'k'	Description
0	First bit is always 0
x	Established TCP connection
y	FIN sent in reverse connection (by the destination)
z	FIN sent in forward connection (by the source)

r_cflags

The r_cflags field contains eight hexadecimal digits that should be interpreted as four bytes of the form ghij. The values of g, h, i and j are interpreted using the tables below.

Byte j is interpreted as eight binary digits of the form PQRSTUVW. If a bit in any position is set to 1, the corresponding value in the table below is assumed.

Bit of byte 'j'	Description
P	Accounting flag (0 if the connection has no accounting)
Q	Accounting flag (0 if the connection has no accounting)
R	Accounting flag (0 if the connection has no accounting)
S	More inspection needed for this connection (has prologue)
T	Reverse connection accepted without going through Rule Base
U	Connection accepted without going through Rule Base
V	One way connection (only the destination sends data)
W	One way connection (only the source sends data)

Byte i may have the following values:

Hexadecimal value	Description
0x66, 0x67	IIOP connections
0x82	clear FTP PORT command
0x83	encrypted FTP PORT command
0x84	FTP PASV command
0x86	RSH stderr connection
0x88	H.245 connection

Hexadecimal value	Description
0x90, 0x91, 0x92, 0x93, 0x94, 0x95	Xtreme connections
0xa1	VDOlive connection
0xa3, 0xa4, 0xa5	RealAudio / RTSP connections
0xa8	RTP connection
0xaa	NetShow connection
0x00	Any other connection

Byte h holds the interface ID (the number of the interface in "fw ctl iflist") of the interface in the direction of the destination.

Byte g holds the interface ID (the number of the interface in "fw ctl iflist") of the interface in the direction of the source.

old_connections table

All connections that were in the connections table during the installation of the security policy are copied into the old_connections table. (The table could be used for various purposes, such as encryption or to reconstruct the key).

Example

```
attributes: expires 3600, keep, sync, kbuf 2
<c0a83005, 0000042d, c7cb473e, 00000017, 00000006; 00004001; 1531/3620>
```

The old_connections table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; different flags (like in the r_ctype connection table); time left/total time>

conn_oneway table

The conn_oneway table is a special table that holds information about connections that are known to be one way only. Connections that are listed in this table are not allowed to operate both ways, but only to the known one way.

Example

```
attributes: refresh, expires 3600
<c7cb471e, 00000014, c0a86e05, 00000549, 00000006; 00000001; 3/55>
```

The conn_oneway table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; rule number; time left/total time>

estab_table table

Sometimes "inverted" entries appear in the log file. In these entries, the source port is a well-known service, and the service (i.e. the destination port) is a random high port.

FireWall–1 times out idle connections after a while and removes them from the connection table. When a TCP connection is erased from the connection table but that connection later receives a delayed reply, the packet is logged by the firewall as dropped (or rejected) since it is unrecognized.

However, FireWall–1 tries to maintain the connection by sending a garbage packet to the destination of the original packet, with the header of the original packet. This step is taken so that if the connection still exists, the internal host will ask the server to re-send, and resume the connection. If the connection is resumed, the only evidence to what has happened is the log entry marking this packet as 'rejected'.

This mechanism operates by default only for a limited period of time after FireWall-1 is started. It is possible to remove these entries by un-checking the checkbox "Log Established TCP Connections" in the Properties window.

Example

```
attributes: expires 30<c7cb4759, c073cd0c, 00000015, 00000543; 28/30>
```

frag_table table

The frag_table table holds information about fragmented packets so the original packet can be reassembled.

Example

```
attributes: expires 20, limit 1000
<c0a83005, c7cb477d, 0000005e, 00000e0e; fee78768; 20/20>
```

The frag_table table uses the following format:

<source IP address, destination IP address, IP protocol, ip_id; ptr; time left/total time>

The ‘ip_id’ value is the value of the IP identification field in the IP header.

The ‘ptr’ value is a pointer to the location where the data fragment is held in kernel memory.

hold_table table

The hold_table table holds packets while the daemon processes them in order to avoid data retransmission.

Example

```
attributes: expires 90, expcall 4234021872 0, limit 100, refresh
<0000005e, 00000e0e; 89/90>
```

The hold_table table uses the following format:

<packet ID, pointer; time left/total time>

The packet ID is a 32-bit integer that is unique and used to identify each packet. The pointer is a pointer to a data structure that contains data on how to handle this packet after the “hold” is over.

pending table

The pending table is a general table that holds information about connections that are not yet fully specified (pending), such as data connections for FTP PASV

Example

```
attributes: refresh, expires 3600, sync, kbuf 1
<c0a83005, 46545053, c7cb47c6, 0000d8f1, 00000006; 00000000, 00004001;
44/60>
```

The pending table uses the following format:

<source IP address, magic number, destination IP address, destination port, IP protocol; encryption key, r_ctype and r_cflags (see r_ctype connection table); time left/total time>

The magic number is an arbitrary number that identifies the VPN-1/FireWall-1 “entity” that recorded this entry, and will need to use the entry later on. Usually the magic number is meaningful when looked upon as 4 ASCII characters.

SAMP tables

sam_blocked_ips table

SAM is an acronym for “suspicious activity monitor” and is a FireWall-1 tool for dynamically blocking IP addresses that are allowed by the Rule Base but which act suspiciously. All newly blocked IP addresses are stored in the sam_blocked_ips table.

Example

```
attributes: expires 2147483647
<c7cb47bb; 00000002, 00000002, 00000001; 2147483386/2147483647>
```

The sam_blocked_ips table uses the following format:

<blocked IP address; IP flags, logging option, action option; time left/total time>

IP flags may have the following values:

IP flag value	Description
0x0001	Block either source or destination
0x0002	Block source
0x0004	Block destination
0x0008	Block source, depending on service
0x0010	Block destination, depending on service
0x0020	Block either source or destination, depending on service
0x0040	Block connection

The logging option may have the following values:

Logging option	Description
0	no log
1	short log, no alert
2	long log, no alert
3	short log, alert
4	long log, alert

The action option may have any combination the following values:

Action option	Description
0x01	Inhibit (do not let additional packets get through)
0x02	Close (terminate existing connections)
0x04	Notify (send a message)
0x08	Cancel (cancel a previous restriction)
0x10	Uninhibit (uninhibit a previously blocked IP address)
0x20	Uninhibit all (uninhibit all previously blocked IP addresses)
0x40	Delete all (delete all previous restrictions)
0x80	Retrieve info (not used)

sam_blocked_servs table

The sam_blocked_servs table holds connections that are blocked by SAM.

Example

```
attributes: sync keep
<c0a80c01, c073cd0c, 00000015, 00000006; 00000002, 00000004>
```

The sam_blocked_servs table uses the following format:

<source IP address, destination IP address, destination port, IP protocol; logging option, action option>

Refer to the tables for the sam_blocked_ips table above to interpret the logging and action options.

License enforcement tables

host_ip_addrs table

The host_ip_addrs table contains the list IP addresses in the FireWall-1 machine (including loopback). The addresses are in Hex format.

Example

```
c7cb4704
7f000001
c7cb4981
c7cb49c7
c7cb49e1
```

forbidden_tab table

Each embedded FireWall-1 has a feature that indicates how many hosts can be located "behind" it (the number of hosts can be unlimited). This limitation is enforced in the Inspect code using the macro COUNT_HOST.

COUNT_HOST records each packet that comes from the internal interface in a table until the limit is exceeded. When that happens an alert is generated. However, rather than issuing an alert on each packet that comes from the same source, the "forbidden" sources are recorded. (Forbidden in the sense that there are X other sources from the internal network that have already been recognized.) Each time an alert is to be generated, the

forbidden table is first checked to see if an alert has already been sent for that source. If the alert has not been sent, the source IP address is recorded and the alert is sent.

Example

```
attributes: expires 300
<c7cb471e; 176/300>
```

The forbidden_tab table format is a list of IP addresses in hexadecimal format.

host_table table

This table holds the IP addresses of internal machines protected by the FireWall. The table only exists where the FireWall license is for a limited number of machines behind the FireWall.

The maximum number of entries in this table is the allowed number of internal machines.

Example

```
Attributes: limit 250
<c0a81f01>
<c0a81f0c>
<c0a81f0e>
```

Logging tables

logged table

The logged table holds all the connections that are all ready logged in order to prevent the same connection from being logged more than once.

Example

```
attributes: expires 62
<00000006, c0a83005, c7cb477d, 0000046e, 00000017, 00000002; 38/62>
```

The logged table uses the following format:

<IP protocol, source IP address, destination IP address, source port, destination port, rule number; time left/total time>

tracked table

The tracked table keeps information for accounting.

Example

```
attributes: refresh, expires 10000, free function 4276413424 11<c0a83005,
00000431, c7cb477d, 00000017, 00000006; 3471650b, 000012ed, 000347c1,
00000001, 00000004, 00000003; 9998/10000>
<00000000, c0a81f01, 00000014, c073cd75, 00000513, 00000006; c073cd75,
00000512, c0a81f01, 00000015, 00000006; 9990/10000>
```

The tracked table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; time, # of packets, # of bytes, rule number, counter, interface; time left/total time>

The first five fields are the “key” fields mentioned above. The time field represents the time measured in seconds since 1/1/1970. The counter runs from 0-10 (0xa), and when it reaches 10 (i.e. every 10th packet) a trap is sent to the daemon to update the live connections log, or a synchronized VPN/FireWall module if such exists. The interface field tracks the interface on which accounting is taking place, to avoid counting packets more than once.

The second entry, which has 0 as the first key, is used to associate a data connection (whose parameters are in the next 5 key fields) with a control connection (whose parameters are the values) for accounting purposes.

trapped table

The trapped table is used to trap connections that need to interact with the daemon while the actual interaction is being made. This avoids forwarding retransmissions while the connection is stalled (for example when negotiating encryption).

Example

```
attributes: expires 10
<c0a83005, 0000061f, c7cb471c, 00000017, 00000006, 00000001; 100/180>
```

The trapped table uses the following format:

< source IP address, source port, destination IP address, destination port, IP protocol, rule number; time left/total time>

dup_con table

The dup_con table is used for special debugging and is not normally used. It holds data on the connections that were chosen to be debug-printed. This table holds the “conn” fields described in The basic structure of a connection in a table entry (above), and a time-out section.

Example

```
attributes: refresh expires 600
<c0a80c01, 00000427, c0a80c2f, 00000015, 00000006; 600/600>
```

domain_cache table

Information about this table will be available in the next update to this document.

arp_table table

Information about this table will be available in the next update to this document.

fwul_table table

Information about this table will be available in the next update to this document.

fwsm_ioctl table

Information about this table will be available in the next update to this document.

synatk_table table

Information about this table will be available in the next update to this document.

fw_route table

Information about this table will be available in the next update to this document.

NAT tables

Address Translation Connection tables

The fwx_forw and fwx_backw tables serve as a connection table for address translated connections for outgoing (forw) and incoming (backw) connections. Each entry holds both the original connection and the translated connection.

fwx_forw table

Example

```
attributes: expires 2147483647, limit 25000, refresh, keep, free function
4276388946 0
<c0a83005, 00000467, c7cb477a, 0000008b, 00000006; c7cb477d, 900027d5,
c7cb477a, 0000008b, 00000000; 3184/3600>
```

The fwx_forw table uses the following format:

<original source IP address, original source port, original destination IP address, original destination port, IP protocol; translated source IP address, translated source port (highest byte is used for flags, translated destination IP address, translated destination port (highest byte is used for flags), TCP sequence structure; time left/total time>

The second destination IP address field listed is the destination of the client. The TCP sequence structure is recorded in case the TCP sequence needs to be changed.

The flags associated with the “source port and flags” and “destination port and flags” fields are:

Flag value	Description
0x10	Established connection
0x20	FIN has been received (2 will also appear in the flags area of the destination port)
0x40	Destination static
0x80	Hide mode
0x08	Reverse UDP (in which case the port will be 0)

fwx_backw table

Example

```
attributes: keep, limit 25000
<c7cb477a, 0000008b, c7cb477d, 000027d5, 00000006; c7cb477a, 0000008b,
c0a83005, 90000467, 00000000>
```

The fwx_backw table uses the same format as fwx_forw, but the entries represent the backward connections. format:

<source IP address, source port, destination IP address, destination port, IP protocol; source IP address, source port and flags, destination IP address, destination port and flags, TCP sequence structure>

Address Translation “partial connections” tables

The fwx_anticipate and fwx_anticipate_rev (reverse) tables are used when translating packets in situations where it is not known on which port the answer will come. When this happens the connections are inserted into these tables with port 0 until the actual packet arrives and the port is known.

fwx_anticipate table

This table hold the translation parameters of data connections that are expected to occur based on existing control connections (e.g. an FTP data connection will be recorded in this table if a PORT or PASV command was detected in the control connection).

Example

```
attributes: expires 2147483647, limit 25000, keep, expcall 4276293796 0
<c0a83005, 00000000, cdd8a363, 00000d6d, 00000006; c0a83005, 00000000, c0a83001,
00000d6d, 00000006; 318/330>
```

The fwx_anticipate table uses the following format:

<anticipated source IP address, anticipated source port, anticipated destination IP, anticipated destination port, anticipated IP protocol; source IP address to translate to, source port to translate to, destination IP address to translate into, destination port to translate into, IP protocol; time left/total time>

The source ports are unknown in this case and are thus set to 0.

fwx_anticpate_rev table

Example

```
attributes: keep, limit 25000
<c0a83005, 00000000, c0a83001, 00000d6d, 00000006; c0a83005, 00000000,
cdd8a363, 00000d6d, 00000006>
```

The fwx_anticipate_rev table uses the following format:

<anticipated source IP address, anticipated source port, anticipated destination IP, anticipated destination port, anticipated IP protocol; source IP address to translate to, source port to translate to, destination IP address to translate into, destination port to translate into, IP protocol>

The source ports are unknown in this case and are thus set to 0.

fwx_alloc table

The fwx_alloc table holds information about the allocation of ports for the translated packets.

Example

```
attributes: keep
<00000000, c7cb477d, 00000006, 00002710; 000027f6>
<c7cb477d, 00000006, 000027d5>
<00000000, c7cb477d, 00000001, 00000258; 0000025c>
```

The fwx_alloc table uses the following formats.

First entry: <0, hiding IP address, IP protocol, first high port used; next high port to be allocated>

The first field is a space holder and is always 0. The first high port to be used is always 10000.

Second entry: <hiding IP address, IP protocol, port already being used>

Third entry: <0, hiding IP address, IP protocol, first low port to be used; next port to be allocated>

The first field is a space holder and is always 0. The first low port to be used is always 600.

fwx_auth table

The fwx_auth table holds the original information of a folded connection, so that back connections can work properly.

Example

```
attributes: expires 300, limit 25000, refresh, keep
<c0a83001, 00000450, c0a83005, 00000635, 00000006; c7cb47e3, 00000017;
286/300>
```

The fwx_auth table uses the following format:

<IP address of the interface of the FireWall-1 machine closest to the client, folded destination port, source IP address, source port, IP protocol; destination IP address, destination port; time left/total time>

The first destination port is the high "folded" port. The second destination port is the original destination port for the service. The source IP address is that of the client and the destination IP address is the final destination.

fwx_frag table

Information about this table will be available in the next update to this document.

VPN tables

Encryption tables

decryption_pending table

During the initialization period of the FWZ scheme, on the responder computer, connections that will need decryption are inserted into the decryption_pending table.

Example

```
attributes: expires 120, kbuf 1;
<c0a83005, 00000456, c7cb477d, 00000017, 00000006; 174/180>
```

The decryption_pending table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

In the case of SecuRemote the format is:

<source IP address, rule number, destination IP address, 0, IP protocol; time left/total time>

encryption_requests table

In the initiation phase of the encryption, connections that are to be encrypted are stored in the encryption_requests table up to the point of actual encryption.

Example

```
attributes: expires 180
<c0a83005, 00000456, c7cb477d, 00000017, 00000006; 174/180>
```

The encryption_requests table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

rejected_encryptions table

Connections that need to be encrypted according to the Rule Base, but cannot be due to problems (wrong scheme, timed out encryption request, failure in key exchange or generation…) are inserted into the rejected_encryptions table.

Example

```
attributes: expires 180
<c0a83005, 00000456, c7cb477d, 00000017, 00000006; 174/180>
```

The rejected_encryptions table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

rdp_table table

The rdp_table table holds RDP (the encryption negotiation protocol) connections in the following particular case. When two computers perform encryption with one another and there is a gateway in the middle that needs to forward these RDP connections, then on the gateway computer, all RDP connections are inserted into this table.

Example

```
attributes: expires 60
<c0a80c01, 000004f9, c7cb47e3, 0000006e, 00000011; 57/60>
<c0a81c0e, c073cd77; 58/60>
```

The rdp_table table uses the following format (these are the values of the original connection):

<source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

In the case of SecuRemote the format is (again, these are the values of the original connection):

<source IP address, destination IP address; time left/total time>

cryptlog_table table

Information about this table will be available in the next update to this document.

SKIP tables

skip_connections table

Each SKIP packet contains the encrypted session key that is decrypted and used to decrypt the packet. In order to optimize the decryption process, the skip_connections table contains the encrypted session key and the non-encrypted session key of a connection. This avoids having to decrypt the session key for each packet.

Example

```
attributes: refresh, expires 180, free function 133280052 0
<4ba107e5, c3298f6d; 802a33bd; 169/180>
```

The skip_connections table uses the following format:

<key1, key2; pointer to key; time left/total time>

The key1 and key2 fields are actually the first and last parts of the same key and are used to identify each key.

skip_key_requests table

The skip_key_requests table holds the requests for skip encryption including the two gateways and their NSIDs.

Example

```
attributes: refresh, expires 60
<00000000, c0a80c1f, 00000000, c073cd1c; 59/60>
```

The skip_key_requests table uses one of the following formats.

In the case of manual IPSec:

<0, source IP address, 0, destination IP address; time left/total time>

In the case of SKIP:

<NSID value of source, source IP address, NSID value of destination, destination IP address; time left/total time>

The NSID values

NSID value	Description
0	None
1	IP
8	MD5

skip_table table

The skip_table table is used for optimization. It holds the shared secret for the two encrypting gateways instead of recalculating it every time.

Example

```
attributes: refresh, expires 86400, free function 133280040 0
<00000000, c7cb4704, 00000000, ce56230b; fc449da8; 85906/86400>
```

The skip_table table uses one of the following formats.

In the case of manual IPSec:

<0, source IP address, 0, destination IP address; shared secret key; time left/total time>

In the case of SKIP:

<NSID value of source, source IP address, NSID value of destination, destination IP address; shared secret key; time left/total time>

Refer to The NSID values table above for descriptions of the possible NSID values.

skip_keyid table

When using SKIP encryption, the pointer to the encryption key in the connections table is actually an entry in the skip_keyid table. The skip_keyid table entry is a pointer to the actual key.

Example

```
attributes: refresh, expires 3600, free function 4233988200 0
<ce56230b, 02010300; fc98ac10; 3106/3600>
```

The skip_keyid table uses the following format:

<destination IP address, encryption methods; pointer to key; time left/total time>

The encryption methods field contains eight hexadecimal digits that should be interpreted as four bytes of the form ghij. Descriptions of each of these bytes are as follows:

Byte	Description (depends on encryption edition (see below)
g	Key encryption method
h	Data encryption method
I	Data Integrity method
j	Always 00

Each of these bytes may contain the following values:

- For VPN+STRONG editions: 0- 3DES, 1- CAST, 2 – RC4-128, 3- DES, 4 – DES-IV32, 5 – RC4-40, 6- RC2-40, 7- DES-40CP, 8- CAST-40, 9- CLEAR
- For VPN+DES editions: 0– 3DES, 1- DES, 2 – DES-IV32, 3 – RC4-40, 4- RC2-40, 5- DES-40CP, 6- CAST-40, 7- CLEAR
- For VPN editions: 0- DES, 1 – RC4-40, 2- RC2-40, 3- DES-40CP, 4- CAST-40, 5- CLEAR
- For 40Bit editions: 0 – RC4-40, 1- RC2-40, 2- DES-40CP, 3- CAST-40, 4- CLEAR

IKE tables

ISAKMP_ESP_table table

Information about this table will be available in the next update to this document.

ISAKMP_AH_table table

Information about this table will be available in the next update to this document.

IPSec tables

manual_table table

The manual_table table is the same as the skip_keyid table, only applied to manual IPSec.

Example

```
attributes: refresh, expires 86400, expcall 4233974528 0
<00000000, 00000101; fc961eb8; 83039/86400>
```

The manual_table table uses the following format:

<0, SPI; pointer to key; time left/total time>

SPI is the IPSec Security Parameters Index – the index of the Security Association used to encrypt/decrypt a datagram.

SA_requests table

Information about this table will be available in the next update to this document.

SPI_table table

Information about this table will be available in the next update to this document.

SecuRemote — client side tables

When running SecuRemote, the machine actually runs a minimal version of FireWall-1. Therefore the connections are managed using the FireWall-1 state tables. The state tables below are special tables that appear only on the SecuRemote client side.

To view the SecuRemote client side tables type:

```
fw tab –u
```

or

```
fw tab –t table_name
```

See the fw tab Syntax and explanation for more options.

enc_timer table

```
attributes: expires 1
<00000001; 1/1>
```

Used by SecuRemote Client:	Yes.
Used by FW daemon:	No.
Keys:	1
Values:	None.
Timeout:	1 sec.
Comments:	Used by the kernel to indicate to the daemon that some decryption/encryption was done during the last 1 second. If such encryption/decryption was done, an entry with a key of 1 will be inserted into the table.

userc_topology table

The userc_topology table holds the topology of the relevant network objects (those that are inside the encryption domains).

Example

```
<c7cb47e3, ffffffff; c7cb4760>
<c0a81e16, ffffffff; c7cb4760>
```

The userc_topology table uses the following format:

<IP address, netmask, encrypting gateways>

Used by SecuRemote Client:	Yes.
Used by FW daemon:	No.
Keys:	<ip, mask, gw>
Values:	None.
Timeout:	None.
Comments:	Used by the client to check whether packets should be encrypted (if they are a part of the topology) or not.

userc_session table

The userc_session table holds the session key for the encryption.

Example

```
attributes: expires 800, free function 4276219426 12
<c0a81e03, c7cb4760; 804c63d8; 632/800>
```

The userc_session table uses the following format:

<client_ip_address, gateway address; key; time left/total time>

The reason that the client IP address is used and not only the gateway address is that most SecuRemote clients are used on a laptop which has a dynamic IP address. So using the client IP address can be beneficial.

Used by SecuRemote Client:	Yes.
Used by FW daemon:	No.
Keys:	<user ip, gw_ip>
Values:	<key>
Timeout:	800 sec
Comments:	Stores negotiated keys between client and firewall on the client side. Note that unless the firewall daemon crashes the session key will always timeout on the client before it times out on the server. If the opposite occurred, communication would not be possible, since the server would not know to decrypt packets from the client.

userc_encapsulating_gateways table

The userc_encapsulating_gateways table holds the addresses of the gateways with which the clients needs to use encapsulation.

Example

```
<c073cd0c>
<c073cd0e>
```

The userc_encapsulating_gateways table uses the following format:

<gateway's IP address>

Used by SecuRemote Client:	Yes.
Used by FW daemon:	No.
Keys:	<gw_ip>
Values:	None
Timeout:	None
Comments:	Used by SecuRemote kernel to decide whether to encapsulate packets. Note that decryption is done based on the IP protocol.

userc_request table

```
attributes: expires 60
<c073cd1c; 55/60>
```

Includes a list of gateways, with which the SecuRemote client has a pending encryption request.

Used by SecuRemote Client:	Yes.
Used by FW daemon:	No.
Keys:	<gw_ip>
Values:	None
Timeout:	60
Comments:	Used by the client to prevent excessive traps to the daemon (indicating that there is currently a negotiation with the gw).

SecuRemote — server side tables

These are the tables used by VPN-1 gateways for the communication with SecuRemote clients.

userc_rules table

The userc_rules table holds a list of rules that are relevant for SecuRemote and a list of IP addresses and sessions key (for optimization).

Example

```
attributes: expires 900, free function 133279992 20
<c0a83005, 00000001; 00000001; 859/900>
<c0a83005, 00000000; 81fc7538; 859/900>
```

The userc_rules table uses the following format:

<client's IP address, rule number; (0 or 1); time left/total time>

or:

<client's IP address, 0; pointer to kernel buffer holding user name; time left /total time>

Used by SecuRemote Client:	No
Used by FW daemon:	Yes
Keys:	<user ip, rule number>
Values:	0 or 1 (intersect with user database or not)
Timeout:	900 sec.
Comments:	Client encrypt rules check this table to see if the connection belongs to SecuRemote clients.

userc_encapsulating_clients table

If in the negotiation phase it was concluded that certain host connections are to be encapsulated, the host IP address and the encapsulating server IP address are inserted into the userc_encapsulating_clients table. This is done after the negotiation for the encryption is over.

Example

```
attributes: refresh, keep, expires 4000
<c0a81e05; c7cb4760; 3998/4000>
```

The userc_encapsulating_clients table uses the following format:

<client IP address; gateway's IP address; time left/total time>

Used by SecuRemote Client:	No.
Used by FW daemon:	Yes
Keys:	<user_ip>
Values:	<gwip>
Timeout:	4000 sec.
Comments:	Used by the firewall kernel when deciding whether to encapsulate packets destined to a user. Note that decryption is done based on the IP protocol.

userc_dont_trap table

When a packet has a destination IP address which is not in the encryption domain, that IP address is added into the userc_dont_trap table so that further communication to that IP address will not be trapped again (for optimization).

Example

```
attributes: expires 10
<c7cb473e; 00000000; 3/10>
```

The userc_dont_trap table uses the following format:

<client's IP address; (0 or 1); time left/total time>

Used by SecuRemote Client:	No.
Used by FW daemon:	Yes
Keys:	<user_ip>
Values:	0 (don't trap) or 1 (trap again only when rule ignores destination restrictions)
Timeout:	10 sec.
Comments:	Used by the daemon to indicate to the kernel that packets coming from a user should not be trapped again because there is already an open RDP connection for those packets.

userc_bind table

The userc_bind table holds the public Diffie-Hellman key of the client for optimizing the specified amount of time in the user properties.

Example

```
attributes: expires 3600, keep, kbuf 1
<4183c5d3, 3a31362a, 9342e2b5; 8029dc98; 3448/3600>
```

The userc_bind table uses the following format:

<client IP address, gateway IP address, username (hashed); user's public key (hashed); time left/total time>

Used by SecuRemote Client:	No.
Used by FW daemon:	Yes
Keys:	<user ip, gw, user name hash>
Values:	<user public key hash>
Timeout:	Configurable on FW daemon. Default: 3600
Comments:	Used to prevent excessive authentication of users. That is, if the user was authenticated once and the relevant values (public key) are still set in this table, the gateway will authenticate the client based on the fact that the client can successfully sign a message sent from the server using this public key.

IPSEC_userc_dont_trap_table table

```
Attributes: expires 15
<c0a80112>
```

This table includes client IP addresses for which a trap was already sent, and there is no need to send an additional one.

Used by SecuRemote Client:	No.
Used by FW daemon:	Yes
Keys:	<user ip>
Values:	None.
Timeout:	15.
Comments:	Used to prevent excessive traps.

userc_request_extended table

Information about this table will be available in the next update to this document.

userc_resolved_gw table

Information about this table will be available in the next update to this document.

userc_DNS_A table

Information about this table will be available in the next update to this document.

userc_DNS_PTR table

Information about this table will be available in the next update to this document.

userc_encrypt_DNS table

Information about this table will be available in the next update to this document.

Security Server and Authentication tables

auth_services table

The auth_services table holds information on the services for which a security server is installed (in the file fwauthd.conf).

Example

```
<00002761, 00000006; 00001180>
<00000050, 00000006, 00000001; 00001184>
<00000050, 00000006, 00000002; 00001185>
```

The auth_services table uses the following format:

<original port to listen on, IP protocol; new actual high port to bind to>

When multiple Security Servers are listening on the same port, an additional field appears after the IP protocol field. The security server field is the ordinal number of the security server (a number between 1 and the total number of security servers) listening on that port.

client_auth table

The client_auth table holds the connections that were authenticated by client authentication and the remaining number of sessions allowed. Entries can be of two formats: standard sign on and specific sign on.

Example

```
attributes: sync expires 60
<00000002, c0a80c01; 00000005, 00000384; 57/60>
<00000002, c0a80c01, 00000001; 00000005, 00000384, 8029dc98; 55/60>
<000000002, c0a80c01, c073cd59, 00000050, 00000006, 00000000; 00000005,
00000384; 53/60>
<000000002, c0a80c01, c073cd59, 00000050, 00000006, 00000000, 00000001;
00000005, 00000384, 8029dc98; 47/60>
```

The client_auth table uses one of the following formats.

In the case of standard sign on (line 1 in the above example):

<rule number, IP address that is now authenticated for access; # of allowed sessions left, seconds until next client authentication ; time left/total time>

Standard sign on entries include the rule number and source IP address as the two keys, and the values are the number of allowed session and the time until the client's next authentication.

In the case of specific sign on (line 3 in the above example):

<rule number, IP address that is now authenticated for access; destination IP address that can be accessed, destination port, IP protocol, RPC connection; # of allowed sessions left, time until user reauthentication; time left/total time>

The RPC connection field is set to 1 if the connection is an RPC connection; otherwise it is set to 0.

Specific sign-on entries have the same values, but the keys are: <rule #, src, dst, dport, ip_p, is_rpc>.

Each of the above entries will have an additional field whose value is 1 if it corresponds to a Single Sign-On using UAM. In that case the entry will also have an additional value which is a pointer to a buffer where the user ID is stored. (Fields 3 and 6 in line 2 above and fields 7 and 10 in line 4 above).

client_was_auth table

The client_was_auth table includes information about the port to which each user-authenticated connection should be folded.

Example

```
attributes: refresh expires 1800
<c0a80e1f, 00000017; 00008235; 1759/1800>
```

The client_was_auth table uses the following format:

<source IP address, original destination port (authenticated service port number); folded destination port; time left/total time>

proxied_conns table

The proxied_conns table helps to keep alive proxied (folded) connections after a reinstallation of policy, by storing the connection information in this table.

Example

```
attributes: keep
<c0a83005, 0000044d, c0a83001, 00000442, 00000006; 00000150, 00000000,
00000000>
<00000000, 00000555, c0a81e16, 00000015, 00000006; 00000150, c0a83005,
0000044d>
```

The proxied_conns table uses the following format.

For the first half of the entry (line 1 above):

<source IP address, source port, destination IP address, destination port, IP protocol; service indicator, 0,0>

The destination IP address is the interface of the FireWall machine that is closest to the source IP address. The service indicator holds the following: three zeros, 4 hex digits for the original destination port, and last digit ("action") which may have the following bits set:

Bit (counting from the right)	Description
1	Encryption (1=connection should be encrypted)
2	Accounting (1=connection should be tracked for accounting)
3	Inside connection (1=connection from the FireWall to itself)

For the second half of the entry (line 2 above):

<0,source port of the final connection, final destination IP address, service port, IP protocol; service indicator, source IP address, source port>

Service indicator (see explanation above)

Source IP (so the entry can be associated with the first one)

Source port (so the entry can be associated with the first one)

autoclntauth_fold table

The autoclntauth_fold table includes information regarding client authentication connections that should be folded. The keys in the table are the source IP address and the service.

Example

```
attributes: expires 60
<c0a80c0e, 00000050; 38/60>
```

The autoclntauth_fold table uses the following format:

<source IP address, destination port; time left/total time>

session_auth table

All connections that were authenticated by session authentication are stored in the session_auth table.

Example

```
attributes: expires 60
<00000001, c0a83005, 00000453, c7cb477d, 00000017, 00000006; 30/60>
<ffffffff, c0a83005, 00000453, c7cb477d, 00000017, 00000006; 30/60>
<fffffffe, c0a83005, 00000453, c7cb477d, 00000017, 00000006; 30/60>
```

The session_auth table uses the following formats.

- For the first part of the entry: (line 1 above):

  <rule number, source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

- For the second part of the entry: (line 2 above):

<-1 (ffffffff), source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

- For the third part of the entry: (line 3 above):

  <-2 (fffffffe), source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

The second and third entries are used to ensure that only one client can work after the authentication. The second entry allows the inbound connection to FireWall-1 and is removed from the table immediately after the authentication is complete.

The third entry ensures that the connection will be able to go through the gateway and is removed from the table as soon as the connection passes the gateway (unless the connection is to the gateway itself in which case the entry will remain until the specified timeout).

session_requests table

All connections that need to be authenticated by session authentication are held in this table until the authentication is completed.

Example

```
attributes: expires 180
<c0a83005, 00000456, c7cb477d, 00000017, 00000006; 174/180>
```

The session_requests table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; time left/total time>

Load balancing tables

check_alive table

The check_alive table holds a list of either load balanced servers or client authentication machines running in wait mode, that should be pinged to verify that they are still working.

Example

```
attributes: expires 60
<c7cb471c,1; 379e4800, 0000003c, 0000001e, 00000001, 32/60>
<c0a83005,1; 379e4800, 0000003c, 0000001e, 00000001, 55/60>
<c0a83017,1; 379e4800, 0000003c, 0000001e, 00000001, 32/60>
```

The check_alive table uses the following format:

<IP address, magic number; last ping time, time to die, recheck, reference count, time left/total time>

magic number – contains ‘1’ for clients in wait mode, or ‘2’ for load balanced servers.

The last ping time is the time (in seconds since 1/1/1970) when the server was last pinged. The time to die is the time until connections are no longer referred to that server if it does not respond. The recheck field is the number of seconds between each two consecutive rechecks. The reference count field tracks how many connections were referred to this server.

logical_requests table

Connections that need to be forwarded to another server as a result of a logical server are stored in the logical_requests table while FireWall-1 determines the correct server to forward the connection to.

Example

```
attributes: expires 180
<c0a83005, 0000061f, c7cb471c, 00000017, 00000006, 00000001; 100/180>
```

The logical_requests table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol, rule number; time left/total time>

logical_servers_table table

The logical_servers_table table holds a list of the logical servers.

Example

```
<c7cb471c; ffffffff, ffffffff>
<c0a83005; ffffffff, ffffffff>
<ffffffff, 00000000; 00000001>
```

The logical_servers_table table uses the following format:

<server IP address; ffffffff, ffffffff>

<ffffffff, 00000000; 00000001> - terminator entry which always appears last in the table

Note that only logical servers that are actually used in rules will appear. Each machine will appear once, even if the machine is used in more than one logical server.

logical_servers_list_table table

The logical_servers_list_table table includes the list of logical servers

Example

```
<c073cd1f, 00000002, 29dc9842; c0a81f0c, c0a81f0e, c0a81f1c>
<c073cd0c, 00000003, 4f77a384; c0a80c1c, c0a80c1f>
```

The logical_servers_list_table table uses the following format:

<logical server IP address, rule number, additional key; IP address of physical server, IP address of physical server…>

In the examples, the first logical server has the IP 192.115.205.31. It is referenced in rule 2, is of type “other” (see explanation in following paragraph) uses round robin, and does not use caching. Its physical servers are 192.168.31.12, 192.168.31.14 and 192.168.31.28. The second logical server has the IP 192.115.205.12. It is referenced in rule 3, is of type “HTTP” (see explanation in following paragraph), uses domain method, and caching.

The additional key field contains eight hexadecimal digits that should be interpreted as four bytes of the form ghij. Bytes g, h and i together form a pointer to the object of the group of physical servers:

The keys are the logical server’s IP address, the rule number, and an additional key whose value is as follows:

- Bits 0-5 of the rightmost byte: The load balancing method, a 6-bit number (server load=0, round trip =1, round robin=2, random=3, domain=4).
- Bit 6 of that byte: ‘1’ for HTTP, ‘0’ for ‘OTHER’.
- Bit 7 of that byte: do we use caching.
- 3 leftmost bytes: pointer to the object of the group of physical servers.

- The values are the IP addresses of the physical servers. The number of values may change, as not all server groups are the same size.

logical_cache_table table

The logical_cache_table table holds cache information for load balancing. Each connection is recorded in the table so it will always be directed to the same security server.

Example

```
attributes: refresh expires 1800 limit 1000
<c0a81201, c073cd1f, 00000017, 00000002; c0a81f0e, 00000017, 00000000;
1790/1800>
<c0a82801, c073cd0c, 00000050, 00000003; c0a80c1c, 00000050, 000080dc;
1794/1800>
<c0a82801, 0029dc98; 18000000; 1793/1800>
```

The logical_cache_table table uses one of the following formats.

If domain caching is not used (lines 1 and 2 above):

<source IP address, logical server's IP address, destination port, rule number; physical server IP address, physical server port, additional value; time left/total time>

Here the destination IP address is the logical server's IP address. The additional value field has a value of 0 for servers of type "other" or holds the in.lhttpd port number for "HTTP".

If domain caching is used (line 3 above):

<Source IP address, logical server unique identifier; flags specifying the physical servers to use; time left/total time>

Specific services tables

icmp_connections table

The icmp_connections table holds state information for ICMP connections.

Example

```
attributes: sync refresh expires 60
<c0a80e1c, 00005e68, c073cd1f; 59/60>
```

The icmp_connections table uses the following format:

<source IP address, ICMP id, destination IP address of the ICMP connection; time left/total time>

h323_tracer_table table

The h323_tracer_table table holds the information regarding the h323 control. Due to the unique nature of the h323 protocol, different ways of implementing it can cause great differences in the appearance of packets. In some cases packets for control and data are different while in other cases the control and data are mixed and their order is different.

This table holds the information about the packet that is expected next, whether control or data.

Example

```
attributes: refresh, expires 900
<c073cd1f, 000005e3, c7cb47c6, 000006bf, 000000006;
```

The h323_tracer_table table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; expecting, data length, direction; time left/total time>

The data length field is the length of the data in bytes. The direction field is either 0 (incoming) or 1 (outgoing). The expecting field is interpreted using the following table:

Expecting value	Description
1	AL_EXPECT_INITIAL_HEADER
2	AL_EXPECT_HEADER
3	AL_EXPECT_MSG
4	AL_IN_HEADER
5	AL_IN_MSG
6	AL_IN_INITIAL_HEADER
7	AL_OUT_OF_SYNC

wf_connections table

The wf_connections table holds a list of win-frame connections (win-frame is a x-server for windows). This table is similar to the “pending” tables but holds only win-frame related information.

Example

```
attributes: refresh, expires 3600, sync
<c0a81f01, 00000684, c073cd85, 000005d6, 00000001; 0005a594; 3599/3600>
```

The wf_connections table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol, connection direction; sequence number; time left/total time>

The connection direction field is either 1 (for a connection from the client to the win-frame server) or 2 (for a connection from the server to the client). The sequence number field is the sequence number of the first packet in each direction. (client to server or server to client)

rtsp_tab table

The rtsp_tab table saves data regarding the RealTime Streaming Protocol (used by RealAudio).

Example

```
attributes: refresh sync expires 60
<c073cd2c, 0000057e, c0a80c01, 0000022a, 00000006; 0000061f; 53/60>
```

The rtsp_tab table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; UDP client port; time left/total time>

Netshow_tab table

Information about this table will be available in the next update to this document.

Cooltalk_datatab table

Information about this table will be available in the next update to this document.

Sqlnet_port_tab table

Information about this table will be available in the next update to this document.

X11_verify_tab table

Information about this table will be available in the next update to this document.

RPC tables

rpc_sessions table

The rpc_sessions table holds information on RPC connections. The key fields are the UDP connection parameters (with 0 in the source port field, as it can be any port), and the value is the RPC program number.

Example

```
attributes: refresh sync expires 40
<c0a81f01, 00000000, c0a81f0c, 00000543, 00000011; 000186a5; 36/40>
```

The rpc_sessions table uses the following format:

<source IP address, source port, destination IP address, destination port, IP protocol; RPC program number; time left/total time>

rpc_serv_hosts table

The rpc_serv_hosts table holds the IP addresses of computers on which the port mapper was successfully contacted. This table is used to implement Stateful inspection for RPC and holds data about the RPC and the "port mapper".

Example

```
attributes: expires 700
<c7cb47e3; 456/700>
<c7cb47c6; 537/700>
```

The rpc_serv_hosts table uses the following format:

<IP address of working port mapper>

rpc_serv table

The rpc_serv table holds the replies for the port mapping requests that are held in the pmap_req table. When an answer connection is entered into this table, it is removed from the pmap_req table. This table is used to implement Stateful Inspection for RPC and holds data about the RPC and the "port mapper".

Example

```
attributes: refresh, expires 800
<c7cb47c6, 00000011, 00000753, 000186c3; 798/800>
```

The rpc_serv table uses the following format:

<source IP address, IP protocol, answer port; program number; time left/total time>

The source IP address is that of the responding server. The answer port is the answer for the port request in the pmap_req table. Refer to the pmap_req table below for information on the program number field.

pmap_req table

The pmap_req table holds the clients' requests to the port mapper for a certain server port. This table is used to implement Stateful Inspection for RPC and holds data about the RPC and the "port mapper".

Example

```
attributes: expires 10
<c0a8cd0c, c7cb47c6, 00000011, 00000753, 5a93f6d6; 000186c3; 5/10>
```

The pmap_req table uses the following format:

<source IP address, destination IP address, port mapper protocol, source port, transaction ID; RPC program number; time left/total time>

The port mapper protocol is either 11 (UDP) or 6 (TCP). The transaction ID is the unique number assigned to any port mapping request. The program number is the unique number of the program whose port was requested. Some typical program numbers are:

Program Number	Description
100001	Rstat
100004	Ypserv
100007	Ypbind
100300	NIS+

Note: Open any RPC service in FireWall-1 to see its program number

pmap_not_responding table

The pmap_not_responding table contains the list of IP addresses of computers on which the port mapper failed to reply.

Example

```
attributes: expires 120
<c7cb47e3; 116/120>
```

The pmap_not_responding table uses the following format:

<IP address which is not replying>

DCE/RPC tables

dcerpc_maps table

The dcerpc_maps table relates to the DCE/RPC port mapper's replies.

Example

```
attributes: sync refresh expires 86400 keep
```

The dcerpc_maps table uses the following format:

Its keys are the Endpoint Mapper's IP address and the GUID requested by the client (which takes 4 fields, since it is 16 bytes long), and the value is the port of the port mapper's response.

See definition of a key in "The basic structure of a connection in a table entry" on page 142)

dcerpc_binds table

The dcerpc_binds table lists the GUID requested in the port mapper connection.

Example

```
attributes: sync refresh expires 3600
```

The dcerpc_binds table uses the following format:

The keys are the connection parameters, and the values are the requested GUID.

See definition of a key in "The basic structure of a connection in a table entry" on page 142

dcerpc_portmapper_requests table

The dcerpc_portmapper_requests table holds requests to the DCE/RPC port mapper that are still not answered.

Example

```
attributes: sync expires 20
```

The dcerpc_portmapper_requests table uses the following format:

Its keys are the connection's parameters and the requested GUID.

See definition of a key in "The basic structure of a connection in a table entry" on page 142

dcom_objects table

The dcom_objects table holds data on the responses to DCOM remote activation requests.

Example

```
attributes: sync refresh expires 86400 keep
```

The dcom_objects table uses the following format:

<source IP address, destination IP address, destination port given by DCERPC portmapper, IP protocol, 4 ClassID fields; time left/total time>

dcom_remote_activations table

Th dcom_remote_activations table holds data on DCOM remote activation requests.

Example

```
attributes: sync refresh expires 60
```

The dcom_remote_activations table uses the following format:

<source IP address, source port, 4 GUID fields; 4 ClassID fields; time left/total time>.

Exchange_notifiers table

Information about this table will be available in the next update to this document.

IIOP tables

iiop_port_tab table

The iiop_port_tab table includes the ports used by the IIOP service (1570, 1571, 2649, 2651).

Example

```
<00000622>
<00000623>
<00000a59>
<00000a5b>
```

The iiop_port_tab table uses the following format:

<IIOP service port number>

iiop_requests table

Information about this table will be available in the next update to this document.

iiop_servers table

Information about this table will be available in the next update to this document.

Static tables (lists)

Static tables are tables with no values. Their entries are inserted during the security policy's compilation and cannot be changed during runtime. They do not time out, and are printed without the angle brackets.

cvp_servers_list table

The cvp_servers_list table contains a list of CVP server IP addresses.

Example

```
c7cb473e
```

The cvp_servers_list table uses the following format:

CVP server IP address

firewalled_list table

The firewalled_list table holds a static list of FireWalled IP addresses.

Example

```
c0a86e01
c7cb471e
```

The firewalled_list table uses the following format:

FireWalled IP address

Object Lists tables

Object Lists tables are tables that correspond to groups that appear in rules.

FireWall-1 binds a list of related hosts, targets, gateways and nets, and gives them a number that corresponds to the rule where they are being used. The host, gateway and net numbers correspond to the rule number in the Rule Base. The target to which those rules apply to has a target_listX number greater by one than all the object lists in that rule.

For example, suppose the rule objects have the following numbers: gateways_list1, host_list2 and host_list3. If there are three rules, then the target_listX will be target_list4.

Below is an excerpt of the `.pf` file – the INSPECT script generated from the policy:

```
-------- gateway_list1 --------
c0a86e01
c7cb471e
-------- host_list2 --------
01010101
02020202
03030303
-------- host_list3 --------
04040404
05050505
06060606
-------- target_list4 --------
 anka
-------- net_list1 --------
199.203.71.0
199.203.156.0
```

radius_servers_list table

The radius_servers_list table contains a list of RADIUS server IP addresses.

Example

```
c7cb47db
```

The radius_servers_list table uses the following format:

RADIUS server IP address

servers_list table

The servers_list table holds the IP addresses of the computers that participate in load balancing. There need not be a rule that involves load balancing for the IP addresses to appear in this table (unlike the logical_servers_table table).

Example

```
c0a83017
c0a83c03
c7cb477d
```

The servers_list table uses the following format:

<server IP address>

tcp_timeouts table

The tcp_timeouts table holds the different timeouts for various TCP services.

Example

```
<00000015; 00001c20>
<00000000; 00000e10>
```

The tcp_timeouts table uses the following format:

<port, timeout>

A port of 0 signifies the default TCP timeout for services not mentioned in the table.

tcp_services table

The tcp_services table holds a list of known TCP ports that are secured and will not be opened insecurely.

Example

```
localhost:
-------- tcp_services --------
00000007
00000009
0000000d
0000000f
00000015
00000017
```

The tcp_services table uses the following format:

<TCP port number>

udp_services table

The udp_services table holds a list of known UDP ports that are secured and will not be opened insecurely.

Example

```
-------- udp_services --------
00000007
00000009
0000000d
00000025
```

The udp_services table uses the following format:

<UDP port number>

Time Objects tables

The following tables are a list of time objects that were created in FireWall-1 Security Policy (this is only an example, as FireWall-1 administrator may create any time objects he or she sees fit).

Examples

```
-------- march_days_in_month --------
00000000
00000001
00000002
-------- April-1-5th_days_in_month --------
00000000
00000001
00000002
00000003
00000004
00000005
-------- april_days_in_month --------
0000000c
0000000d
0000000e
0000000f
00000010
```

ufp_servers_list table

The ufp_servers_list table holds a list of UFP server IP addresses.

Example

```
c7cb473e
```

The ufp_servers_list table uses the following format:

<UFP server IP address>

table_target_list tables

The table_target_listX is a table that holds information about address translation rules. Used when a single rule performs one or more address translations.

Example: table_target_list8

```
<00010001, 00000001, c0a86e05, c0a86e05, c7cb471e, 00000000, 00000000>
```

The table_target_list table uses the following format:

<index number, rule type, first IP address in range, second IP address in range, first hiding IP address, always 00000000- follows a group of five fields (fields one to five and the zero field can repeat), always 00000000 - indicates the final field of the entry>

In the case of single-host address translation, the first IP address in range equals the second IP address in range. The rule types are as follows:

Rule type	Description
0x0	End of NAT rule
0x1	FWXT_HIDE (hide tranlatation)
0x2	FWXT_SRC_STATIC (source static translation)
0x202	FWXT_DST_STATIC (destination static translation)
0x302	FWXT_DPORT_STATIC (port translation)

Appendix B: Object.C Properties in VPN-1/FireWall-1 4.0

The Properties section of the $FWDIR/conf/objects.C file

The `objects.C` file includes a section of properties whose values affect the VPN-1/FireWall-1 behavior. These properties exist in addition to network objects, server objects, service objects, time objects and other miscellaneous data. The section under consideration begins with the line:

```
:props (
```

Immediately following, are lines with the format:

```
:property (value)
```

Note: The blank space preceding the '`(`' is required on the "`props`" line and each "property" line. Omitting the blank space will result in a failure to load the security policy. In certain cases the parentheses may be omitted, but it is best to use them in all cases to avoid any possible mistake.

To modify any of the properties listed in the table below, do the following:

1. Close all VPN-1/FireWall-1 GUI clients.
2. Edit the `$FWDIR/conf/objects.C` file. (Use a simple text editor such as Notepad. Do not use a word processor).
3. Search for the desired property.
4. If the property is found, change its value to the desired value.
5. If the property is not found, add a new line after the "`props`" line. Use the format shown above to list the new property and assign it a value.
6. Save the changes to the `objects.C` file.
7. Reload the security policy.
8. For properties that involve the security servers, VPN-1/FireWall-1 must be restarted.

If the property is a Boolean property (i.e. ONLY if its value is either 'true' or 'false'), use the command '`fw config <property> put <true|false>`' rather than edit the `objects.C` file.

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
acceptdecrypt	1	Accept encrypted messages on 'accept' rules and decrypt them (true) or not (false)	TRUE
add_ntgroups	0	Query the Windows NT domain controller for user groups (true) or not (false)	FALSE
addresstrans	0	This property is no longer used	TRUE
adtr_skip_routing_msg	1	This property is no longer used	FALSE
alertcmd	1	Command to issue in case of alerts. May contain the name of any OS command or executable file	Fwalert
allow_all_options	0	Allow all telnet options (true) or not (false)	FALSE
allow_clear_gettopo	1	Topology download to SecureRemote clients may use cleartext as well (true) or only SSL (false).	TRUE

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
allow_encryption_outgoing_first	0	Allow encryption rules even if "allow outgoing packets" is set to "first" (true) or send outgoing packets unencrypted in that case (false)	FALSE
allowed_telnet_option	0	The number of telnet option to be allowed (between 0 and 40. Use this property multiple times to allow multiple options)	
as_failure_limit	0	Maximum number of retries for authentication with Check Point RADIUS server	5
as_radius_free_type	0	RADIUS types that Check Point authentication server knows about, in addition to the standard ones. Use this property multiple times to allow multiple RADIUS types	40
au_connect_timeout	0	The interval (in seconds, ranging from 1 to MaxInt) until the security server will try to connect again after there is no reply.	10
au_timeout	1	The interval (in minutes, ranging from 1 to 800) until the user is prompted again for authentication.	15
automatically_open_ca_rules	1	Use the automatic client authentication as in FireWall-1 version 3.0 (true) or not (false). This feature is made obsolete by the automatic client authentication of 4.0, and is not to be used in VPN-1/FireWall-1 4.0 or above.	FALSE
block_reverse_tcp	1	This property is no longer used	FALSE
block_reverse_tcp_p	1	This property is no longer used	First
block_reverse_udp	1	This property is no longer used	FALSE
block_reverse_udp_p	1	This property is no longer used	First
ca_matchbyname	1	Match destination field in fully automatic CA rules by name (true) or by IP address (false)	FALSE
ca_wait_mode	1	Leave the client authentication session open after authenticating, and when the session closes - terminate the authenticated session (true) or close session automatically once the client authenticates (false)	FALSE
clnt_auth_msg	0	Client Authentication message text	"Check Point FireWall-1 Client Authentication Server running on"
control_back_compatibility	1	Use backward compatibility between FireWall-1 versions 3.0 and 4.0 (true) or not (false)	FALSE
cooltalkenable	0	Enable CoolTalk (true) or not (false) (this property is relevant for FireWall-1 version 3.0 or backward compatibilty only)	TRUE
default_track	1	Default track for user authentication failure (may be Auth (=logging only), AuthAlert (=logging and alerting) or blank (=no action))	AuthAlert
domain_tcp	1	Allow domain-tcp (true) or not (false)	TRUE

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
domain_tcp_p	1	Where in the policy to allow domain_tcp (first, last or before last)	first
domain_tcp_router	1	Allow domain-tcp in access lists (true) or not (false)	TRUE
domain_tcp_router_p	1	This property is no longer used	first
domain_udp	1	Allow domain-udp (true) or not (false)	TRUE
domain_udp_p	1	Where in the policy to allow domain_udp (first, last or before last)	first
domain_udp_router	1	Allow domain-udp in access lists (true) or not (false)	TRUE
domain_udp_router_p	1	This property is no longer used	first
enable_fastpath	1	Pass established packets without checking them against the rulebase (true) or check them (false)	FALSE
enable_objects_check	1	This property is no longer used	TRUE
enable_tcprpc	1	Enable RPC over TCP (true) or not (false)	FALSE
encryption_kernel_logging	1	Log encryption kernel events (true) or not (false)	TRUE
established	1	This property is no longer used	TRUE
established_p	1	This property is no longer used	first
established_router	1	Accept established TCP connections in access lists (true) or check them against the list (false)	TRUE
established_router_p	1	This property is no longer used	first
exportableskip	1	Generate 512-bit SKIP keys in addition to 1024-bit SKIP keys (true) or not (false)	FALSE
ftp_allowed_cmds	1	Allowed FTP commands, in a quoted string, separated by blanks	"ABOR ACCT ALLO APPE BYE BYTE CDUP CWD DELE FIND FW1C HELP LIST MACB MAIL MDTM MKD MLFL MODE MRCP MRSQ MSAM MSND MSOM NLST NOOP PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR RNTO SITE SIZE SOCK STOR STOU STRU SYST TYPE USER XCUP XCWD XMD5 XMKD XPWD XRMD"
ftp_dont_accept_site_on_login	0	Pass SITE command(true) or not (false)	FALSE
ftp_dont_check_random_port	0	Allow using TCP service ports in FTP data connections (true) or not (false)	FALSE

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
ftp_listen_timeout	0	Timeout interval (in seconds, between 1 and MaxInt) if a peer of the FTP security server does not connect to a port opened for that peer	60
ftp_msg	0	FTP security server welcome message text	"Check Point FireWall-1 Secure FTP server running on"
ftp_msg_max_lines	0	Maximum number of lines in the FTP server's welcome message (between 0 and MaxInt)	100
ftp_use_cvp_reply_safe	0	Allow the CVP server to send data before the reply (true) or not (false)	FALSE
ftpdata	1	Allow FTP data connections (true) or not (false)	TRUE
ftppasv	1	Allow FTP PASV connections (true) or not (false)	TRUE
fw_ignore_domain_rules	0	Ignore rules with domain in source when matching rulebase via security servers (true) or resolve domain names and match (false)	FALSE
fw_ignore_session_rules	0	Ignore session authentication rules when matching rulebase via security servers (true) or drop connections that match these rules (false)	FALSE
fw_light_verify	0	Do not check for rulebase overlaps during rulebase verification (true) or perform the full check (false)	FALSE
fw_listen_queue	1	The length of the listen queue for every security server being run (between 0 and MaxInt)	200
fw1_enable_p	1	Where are the control connections enabled (first, last or before last)	first
fw1enable	1	Enable VPN-1/FireWall-1 control connections (true) or not (false)	TRUE
fwfrag_limit	0	Maximum number of fragments in a packet (may range from 1 to MaxInt)	1000
fwfrag_minsize	0	Minimum size for a fragment (in bytes)	0
fwfrag_timeout	0	Timeout interval (in seconds) for fragment reassembley of one IP packet (may range from 0 to MaxInt)	20
fwldap_cachesize	1	The number of LDAP users that will be cached (may range from 0 to MaxInt)	100
fwldap_cachetimeout	1	Timeout interval on cached LDAP users (in seconds, may range from 0 to MaxInt)	900
fwldap_displaydn	1	Display the user's DN at login (true) or not (false)	FALSE
fwldap_passwordcheckmethod	1	Check if the password has expired (true) or not (false)	1
fwldap_passwordexpiration	1	Days before LDAP password expires (between 0 and MaxInt)	90
fwldap_requesttimeout	1	Timeout on LDAP requests (in seconds, between 0 and the TCP timeout)	20

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
fwldap_sizelimit	1	Number of entries account unit can return (between 0 and MaxInt)	10000
fwldap_useldap	1	Use LDAP Account management units (true) or not (false)	FALSE
fwsynatk_ifnum	1	Which interface does SynDefender work on (the value is the number of the interface as it appears in the output of “fw ctl iflist”. –1 means all interfaces)	-1 (all)
fwsynatk_max	1	Maximum number of concurrent half open connections (between 500 and 10035)	5000
fwsynatk_method	1	Which SynDefender method is used (0=none, 1=relay, 2=active or 3=passive)	0 (none)
fwsynatk_timeout	1	How long until SynDefendef gives up on receiving ACK (in seconds, between 1 and 60)	10
fwsynatk_warning	1	Send a log message for SYN attacks (1) or not (0)	1
fwz_encap_mtu	1	Backward compatibility with FireWall-1 version 3.0 when using FWZ + Encapsulation (1) or not (0)	1
gatewaydir	1	Direction on interface where filtering is done (inbound, outbound or eitherbound)	inbound
http_allow_double_slash	0	Allow '//' in the middle of the URL(true) or not (false) (needs to be used in conjunction with 'scheme' or 'http_use_default_schemes' properties)	FALSE
http_allow_ranges	0	Allow range headers(true) or not (false)	FALSE
http_avoid_keep_alive	0	Allow only one request per connection (true) or more (false)	FALSE
http_block_java_allow_chunked	0	Allow HTTP 1.1 chunks even when Java is blocked (true) or not (false)	FALSE
http_cvp_allow_chunked	0	Allow HTTP 1.1 chunks even when CVP is used (true) or not (false)	FALSE
http_disable_ahttpdhtml	0	This property is no longer used	FALSE
http_disable_automatic_client_auth_redirect	0	Disable automatic client authentication redirection (true) or enable it (false)	FALSE
http_disable_cab_check	0	Do not search for Java classes in CAB files (true) or search them (false)	FALSE
http_don’t_handle_next_proxy_pw	0	Leave the password in the proxy password field for the next proxy (true) or erase it (false)	FALSE
http_erase_ftp_links	0	Erase FTP links from HTTP traffic (true) or leave them (false)	FALSE
http_erase_port_cmd	0	Erase FTP PORT commands from HTTP traffic (true) or leave it (false)	FALSE
http_failed_resolve_timeout	0	Timeout interval to resolve the server's address, in seconds	900

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
http_force_down_to_10	0	Force HTTP 1.1 connections into HTTP 1.0 (true) or not (false)	FALSE
http_handle_proxy_pw	0	The next proxy may (true) or may not (false) ask for a password	TRUE
http_log_every_connection	0	Log every HTTP connection (true) or avoid logging connections that are too close in time to each other (false)	FALSE
http_max_auth_password_num	0	Maximum number of authentication sessions	1000
http_max_auth_redirect_num	0	Maximum number of redirected sessions	1000
http_max_connection_num	0	Maximum number of connections handled by the HTTP Security Server	4000
http_max_header_length	0	Maximum length of HTTP header	1000
http_max_header_num	0	Maximum number of HTTP headers	500
http_max_held_session_num	0	Maximum number of sessions that can be simultaneously in HOLD state	1000
http_max_realm_num	0	Maximum number of realms the HTTP security server can handle	1000
http_max_server_num	0	Maximum number of HTTP servers the HTTP Security Server can handle	10000
http_max_session_num	0	Maximum number of simultaneous sessions (0 means infinite)	0 (infinite)
http_max_url_length	0	Maximum length of URL	2048
http_next_proxy_host	1	What is the host of the HTTP next proxy (IP address or resolvable name)	
http_next_proxy_port	1	What is the port of the HTTP next proxy (between 1 and 65535)	
http_no_content_length	0	Do not send the content length to the client (true) or do send it (false)	FALSE
http_old_auth_timeout	0	Time interval in seconds that an old password is accepted for authentication after it expired	0 (never)
http_process_timeout	0	Time interval in seconds that the ahttpd can be active until it is terminated	32400
http_query_server_for_authorization	0	Send HEAD request before answering the client (true) or do not send HEAD request (false)	FALSE
http_redirect_timeout	0	Timeout interval in seconds for redirection of an HTTP session	300
http_servers	0	Set of predefined HTTP servers (use the GUI to edit this property, and do not edit it through the objects.C)	
http_session_timeout	0	Maximum time interval in seconds for an HTTP session to be idle	300

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
http_skip_redirect_free	0	Free memory when redirecting a connection for authentication, to prevent memory leaks (true) or avoid freeing session's memory (false)	TRUE
http_sup_continue	0	Send HTTP 1.1's "continue" command to the client (true) or not (false)	FALSE
http_use_cvp_reply_safe	0	Allow the CVP server to send data before the reply (true) or not (false)	FALSE
http_use_default_schemes	0	Allow the default schemes (prospero, gopher, telnet, finger, mailto, http, news, nntp, wais, file and ftp) to preceed a '//' in the query field of a URL (true) or do not allow any schemes unless specifically stated (false)	FALSE
http_use_host_h_as_dst	0	Redirect by name (true) or by IP address (false) in partial CA	FALSE
http_use_proxy_auth_for_other	0	Support agent other than Mozilla or Internet explorer (true) or not (false)	TRUE
http_weeding_allow_chunked	0	Allow HTTP 1.1 chunks even when HTML weeding is used (true) or not (false)	FALSE
icmpcryptver	1	Encrypt ICMP inplace(0) or not (1)	1
icmpenable	1	Enable stateful inspection & accept for ICMP (true) or accept ICMP only if rulebase allows it specifically (false)	TRUE
icmpenable_p	1	Where to enable ICMP in the policy (first, before last, or last. Use last to enable stateful inspection for ICMP, but accepting it only when the rulebase specifically allows it)	before last
icmpenable_router	1	Enable ICMP in access lists (true) or not (false)	TRUE
icmpenable_router_p	1	Where to enable ICMP in the access lists (first, before last or last)	before last
imap_msg	0	Default message text for IMAP daemon	" * OK CheckPoint FireWall-1 Authenticated Imap Server running on"
iphoneenable	0	Enable Iphone (true) or not (false) (this property affects only FireWall-1 version 3.0 or backward compatibility of 4.0 with 3.0)	TRUE if Iphone appears in the rulebase, FALSE otherwise
ipoptslog	1	Default track for packets with IP options ("IP Options" (=logging only), "IP Options Alert" (=logging and alerting) or blank)	
ipsec_spi_alloc_max	0	Highest SPI value in hex (used in VPN-1/FireWall-1 version 4.0 SP7, 4.1 SP2 and above)	10000
ipsec_spi_alloc_min	0	Lowest SPI value in hex (used in VPN-1/FireWall-1version 4.0 SP7, 4.1 SP2 and above)	100

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
isakmp.encryption	0	Default client encryption scheme, if not specified by the SecureRemote user (“DES”, “DES-IV32”, “CLEAR” or “RC4-40”	“DES”
isakmp_logging	1	Log IKE negotiation (true) or not (false)	TRUE
isakmpphase1reneg	1	Time interval after which the ISAKMP session key is changed (in minutes, between 5 and 525600)	10080
isakmpphase2reneg	1	Time interval after which the IPSec session key is changed (in seconds, between 120 and 86400)	3600
isakmpphase2renegkbytes	1	Number of kilobytes transferred until the IPSec session key is renegotiated (0 means infinite)	0 (infinite)
lbalanced_load_history_percent	1	The effect (in percent) history is taken into account in load balancing (between 0 and 100)	0
lbalanced_load_period_wakeup_sec	1	This property is no longer used	20
lbalanced_period_wakeup_sec	1	How often the load agent is queried (once every how many seconds)	30
lbalanced_roundtrip_history_percent	1	The effect (in percent) roundtrip history is taken into account in load balancing (between 0 and 100)	85
liveconns	1	Use live connections (true) or not (false)	FALSE
load_service_port	1	The port of the load agent (0 means random high port)	0
log_established_tcp	1	Should established TCP packets be logged if rulebase says so (true) or not (false)?	TRUE
log_implied_rules	0	This property is no longer used	
log_keepalive_minute_to	0	Time interval in minutes to check that all the log connections are indeed active	300
log_switch_size	0	This property is no longer used	
loggrace	1	Log grace period (in seconds, between 0 and 90) to avoid repetetive logging of retransmissions	62
logical_servers_timeout	0	Time interval (in seconds) to check if the logical server is alive	60
looptcp	1	This property is no longer used	TRUE
looptcp_p	1	This property is no longer used	first
loopudp	1	This property is no longer used	TRUE
loopudp_p	1	This property is no longer used	first
mailcmd	1	Command to issue for mail alerts May contain the name of any OS command or executable file	/bin/mailx -s 'FireWall-1 Alert' root
manualmaxspi	1	Highest SPI value (only through VPN-1/FireWall-1 version 4.0 SP-6 and 4.1 SP-1. No longer used in later versions)	0x10000

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
manualminspi	1	Lowest SPI value (only through VPN-1/FireWall-1 version 4.0 SP-6 and 4.1 SP-1. No longer used in later versions)	0x100
maxprocess	1	This property is no longer used	256
nat_hashsize	0	Hash size for NAT tables. May be any power of 2 up to 65536	8192
nat_limit	0	Limit for NAT tables (between 0 and 50000)	25000
new_ftp_interface	0	Use the new FTP interface (True) or the old method that uses '@'s (False)	FALSE
outgoing	1	Allow outgoing connections (true) or match them by the rulebase (false)	TRUE
outgoing_p	1	Where in the rulebase to allow outgoing connections (first, before last or last)	last
pagetimeout	1	This property is no longer used	20
pmap_connect_timeout	1	Default timeout for connecting to the RPC portmapper, in seconds	30
pop3_daemon	0	Path on POP3 daemon on the local machine	
pop3_server	0	Default POP3 server	
prohibited_telnet_option	0	The numbers of telnet options to be prohibited (between 0 and 40). Use this property multiple times to prohibit multiple options.	
prompt_for_destination	1	Forcing non-transparent mode (as in pre-FireWall-1 version 3.0) (true) or enable transparent authentication (false)	FALSE
psswd_min_length	1	Minimum length of password for LDAP users, in characters	2
psswd_min_num_of_lowercase	1	Minimum number of lowercase letters in password for LDAP users	0
psswd_min_num_of_numbers	1	Minimum number of numbers in password for LDAP users	0
psswd_min_num_of_symbols	1	Minimum number of symbols (non-alphanumeric) in password for LDAP users	0
psswd_min_num_of_uppercase	1	Minimum number of uppercase letters in password for LDAP users	0
radius_connect_timeout	0	Timeout interval until next attempt to connect to the RADIUS server, in seconds	120
radius_ignore	0	Ignore RADIUS attributes that are not defined in RFC 2138 and RFC 2139. The value is a list of RADIUS attributes to ignore. Consult Check Point support if you want to modify this field.	
radius_retrant_num	0	Maximum number of connection attempts to the RADIUS server	2
radius_retrant_timeout	0	Timeout interval for each RADIUS server connection attempt, in seconds	5

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
radius_send_framed	1	Send the framed host (source IP of the connection) to the RADIUS server	FALSE
radius_user_timeout	0	Timeout interval for the the user to respond to a RADIUS challenge, in seconds	600
raudioenable	0	Enable RealAudio (only in FireWall-1 version 3.0 or backward compatibility of 4.0 with 3.0)	true if "RealAudio" appears in the rulebase, false otherwise.
remote_auth_group	0	Name of user group which uses the internal RADIUS server	NULL
remote_auth_server	0	Name of VPN-1/FireWall-1 internal RADIUS server	NULL
resolver_1	1	This property is no longer used	sys (current sysytem settings)
resolver_2	1	This property is no longer used	None
resolver_3	1	This property is no longer used	None
resolver_4	1	This property is no longer used	None
retries	1	Maximum number of retries for address resolution	1
rip	1	Enable RIP (true) or not (false)	TRUE
rip_p	1	Where to enable RIP in the policy (first, last or before last)	first
rip_router	1	Enable RIP in access lists (true) or not (false)	TRUE
rip_router_p	1	Where to enable RIP in the access lists (first, last or before last)	first
rlogin_msg	0	Arlogind welcome message	"Check Point FireWall-1 authenticated Telnet server running on"
rpcenable	1	Enable RPC (true) or not (false)	TRUE
rshstderr	1	Allow rsh connections to stderr (true) or not (false)	FALSE
scheme	0	Which HTTP schemes may appear before the // (the possible values are names of HTTP schemes, or any other sequences of letters that are acceptable before the “//”)	
securid_timeout	0	Timeout interval for connections with ACE server (in seconds)	300
skey_mdmethod	0	This property is no longer used	
skipmaxbytes	1	Number of bytes transferred until the SKIP key is changed	1048576
skipmaxtime	1	Time interval in seconds until the SKIP key is changed	120
smtp_add_received_header	0	Add a "Received" header (true) or not (false)	FALSE

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
smtp_exact_str_match	0	Insist that header fields match exactly (true) or allow header fields with no ":" (false)	FALSE
smtp_limit_content_buf_size	0	Forbid content type headers longer than 4K (true) or allow them (false)	TRUE
smtp_msg	0	Asmtpd welcome message	""
smtp_multi_cont_type	0	Allow MIME nesting (true) or not (false)	FALSE
smtp_rfc821	0	Insist on <> around the email address (true) or not (false)	TRUE
smtp_rfc822	0	Insist on RFC822 compliancy (true) or not (false)	TRUE
smtp_strip_active_tags	0	Strip activeX by default (true) or not (false)(resource may override this)	FALSE
smtp_strip_applet_tags	0	Strip Java by default (true) or not (false)(resource may override this)	FALSE
smtp_strip_ftp_tags	0	Strip FTP links by default (true) or not (false)(resource may override this)	FALSE
smtp_strip_port_tags	0	Strip PORT commands by default (true) or not (false)(resource may override this)	FALSE
smtp_strip_script_tags	0	Strip JavaScript by default (true) or not (false)(resource may override this)	FALSE
sn_connect_timeout	0	Time interval in seconds to try to connect the agent after failure	10
sn_timeout	0	Timeout on connecting to the agent, in seconds	120
snauth_old_clients_message	0	Message text displayed to users of old session agents.	"FireWall Module does not support non-encrypted connection. Please update your agent software."
snauth_protocol	0	Support for old versions of the session agent? Support for SSL? (none=yes,no; ssl=no,yes; ssl+none=yes,yes)	No default value exists. If the property does not appear neither old versions of the session agent nor SSL are supported
snk_agent_id	0	The agent ID of the AXENT defender	""
snk_agent_key	0	The agent key of the AXENT defender	""
snk_server_bkp_ip	0	The backup IP address of the AXENT defender	""
snk_server_ip	0	The IP address of the AXENT defender	""
snk_timeout	0	Timeout interval for the connection to the AXENT defender	20
snmptrapcmd	1	Command to issue for SNMP traps	"snmp_trap localhost"
spoofalertcmd	1	Command to issue for IP spoofing alerts	"fwalert"

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
sso_resolve_src	0	Resolve the source IP address when logging SSO Client Authentication (true) or not (false)	FALSE
stack_size	0	Size of INSPECT stack in bytes	1024
suppress_dont_echo	0	Suppress the "don't echo" property of telnet (true) or allow it (false)	FALSE
tcp_reject	0	Perform 'reject' for TCP packets when rulebase is configured to do so (true) or perform ‘drop’ (false)	TRUE
tcpendtimeout	1	Timeout interval in TIME_WAIT until we close a TCP connection (in seconds)	50
tcpestb_grace_period	0	For how many seconds after 'fwstart' do we operate the TCP established mechanism (0=never, -1=always, 37= 37 seconds, etc.)	0
tcpstarttimeout	1	Time interval to wait for a SYN/ACK in SYN_SENT (in seconds)	60
tcptimeout	1	Time interval to wait on an idle TCP connection (in seconds)	3600
telnet_msg	0	Atelnetd welcome message text	"Check Point FireWall-1 authenticated Telnet server running on"
timeout	1	Time interval to wait for address resolution (in seconds)	10
udp_reject	0	Perform 'reject' for UDP packets when rulebase is configured to do so (true) or perform ‘drop’ (false)	TRUE
udpreply	1	Enable reply packets in a two-way UDP communication (true) or inspect reply according to the rulebase (false).	TRUE
udptimeout	1	Time interval to wait on an idle UDP connection (in seconds)	40
undo_msg	0	Do not send the VPN-1/FireWall-1 standard greeting message(true) or send it (false)	false
use_zero_buf_len	0	Reset the S_TO_C buffer length always(0), only for FTP over HTTP(1), or never (2)	0
useralertcmd	1	Command to issue for user-defined alerts	“fwalert”
userauthalertcmd	1	Command to issue for user authentication failure	“fwalert”
userc_bind_user_to_ip	0	Allow same username to connect from different IP addresses and enable SecureRemote clients with DHCP (true) or not (false)	false
userc_crypt_ver	1	Backward compatibility with previous versions for client-encrypting rsh and sqlnet (0-old, 1-new)	1
userc_ike_nat	1	Support NATed SecureRemote clients with IKE (true) or not (false)	FALSE
userc_nat	1	Support NATed SecureRemote clients with FWZ (true) or not (false)	FALSE

Property	Property always appears in object.C ? (1 = yes, 0 = user has to add entry)	Explanation	Default Value
vdolivenable	0	Enable VDOlive (only for FireWall-1 version 3.x or backward compatibility with version 3.x)	true if vdolive appears in the rulebase, false otherwise.
vlog_switch_size	1	Size in KBytes that the active connections log is automatically switched (i.e. the current connections log is closed and a new one is opened).	10
write_acct_to_db	1	This property is no longer used	FALSE

Appendix C: Log Viewer "info" Messages

In This Chapter:

Messages in the 'info' column of the log viewer.....190

More Information.....192

HTTP Security Server "Reason" Messages 192
Log Encryption Error Messages 192
SecuRemote Error Messages 192

Messages in the 'info' column of the log viewer

The 'info' column of the log viewer includes all the fields which do not belong in any other column of the log file. Some of the VPN-1/FireWall--1 log fields do not have a matching column in the log viewer. If such a field is empty, it will not be displayed, but if it is not empty it will be displayed in the ‘info’ column of the log viewer.

Therefore, the info column could look as follows:

```
"len 44 resource http://www.checkpoint.com/"
```

Which means that the 'len' field contains the value '44', and the 'resource' field contains the value 'http://www.checkpoint.com/'.

The following Log fields do not have matching columns:

Log fields which do not have matching columns

FIELD	MEANING
Agent	The name of the mail server from which SMTP mail has been received.
Alert	The type of alert generated: "alert", "snmptrap", "mail", "useralert", "spoofalert" or "userauthalert".
cat_server	The name of the UFP server.
Category	The UFP category which matches a certain URL.
Decryption failure:	Message with the reason why decryption failed. The list of possible messages appears on pages 259-267 of the VPN Guide, Check Point 2000 (pages 133-139 of the VPN-1 User Guide, version 4.0)
Encryption failure:	Message with the reason why encryption failed. The list of possible messages appears on pages 259-267 of the VPN Guide, Check Point 2000 (pages 133-139 of the VPN-1 User Guide, version 4.0)
Expire	The SAM request will expire at this time
File	In FTP account logs, the name of the file downloaded/uploaded by FTP.
From	The "from" address of the SMTP mail message, after a possible translation.
h_len	The length of the IP header.
Icmp-type	The ICMP type of an ICMP packet.
Icmp-code	The icmp code of an icmp packet.

FIELD	MEANING
ip_vers	Contains the I.P. version (normally 4).
Key update for	The name of the module for which a key update has occurred.
Len	Contains the length of the packet, when 'long' logging is used.
License violation detected	This field exists when a license violation is detected. Contains the list of internal addresses (one address for each log record) in ip format (e.g. 192.168.160.1).
Message	For a log of a syn attack, specifies the nature of the attack. Could be either "syn -> syn-ack -> rst" or "syn -> syn-ack -> timeout".
Methods:	Contains three components separated by commas. The first is the algorithm used to generate the session key, the second is the algorithm used for the entire session, and the third is the hashing algorithm (e.g. "fwz, des, md5").
Orig_from	The "from" address of the SMTP mail message, before a possible translation.
Orig_to	The "to" address of the SMTP mail message, before a possible translation.
Packets	The number of packets transferred in a session. Used for accounting and live connections.
Reason	Contains the authentication message in authentication rules. A list of the messages can be found on page 507 of the Check Point 2000 Administration Guide (page 56 of the VPN-1/FireWall--1 Architecture and Administration User Guide, Version 4.0). Authentication attempts may be denied for any of the 8 reasons specified. In addition, you can also get the successful authentication message ("authenticated by" followed by the scheme - radius, axent, s/key, securid, os password or VPN-1/FireWall--1 internal password).
Res_action	In ftp/http account logs, contains the direction of the file transfer ("get" or "put").
Resource	In http account logs, contains the url accessed.
Request	The type of a sam request: “inhibit” or “uninhibit”.
Rpc-prog	Contains the rpc program number for rpc rules.
Scheme:	The encryption scheme used ("fwz", "skip", etc.)
Signed by	The certificate authority used to sign a certain key sent to a firewall module.
Start_time	The time the connection started. Used for accounting.
SPI	Contains the ipsec spi.
Sys_msgs	Contains one of the following: "started sending log to local host", "security policy uninstalled", "installed <name of security policy>".
Target	The host for which the “inhibit” or “uninhibit” sam request was made.
To	The "to" address of the smtp mail message, after a possible translation.
Error notification	From …, to …, cause of errors in resending e-mail from mail dequeuer to mail server (connection failed, no disk space on mail server, etc.) .
ISAKMP Log	Completion of Phase 1, encryption algorithm/hash algorithm, Causes of any Phase 1 errors.
Negotiation Id	Host(1) negotiation id Host(2) negotiation id.

FIELD	MEANING
Command	The command given in a session. Used for live connections.
Success reason:	Reason for decryption: Decrypt by accept_rip rule Decrypt by accept_domain_udp rule Decrypt by accept_domain_tcp rule Decrypt by accept_icmp rule Decrypt by accept rule Decrypt by user authentication rule Decrypt by client authentication rule Decrypt by session authentication rule

More Information

HTTP Security Server "Reason" Messages

For a list of reason messages when HTTP Authentication fails, see “Reason Messages”:

- FireWall-1 4.0 Architecture and Administration book of the User Guide, page 56
- VPN-1/FireWall-1 4.1 SP1 (Check Point 2000) Administration Guide page, page 507

Log Encryption Error Messages

For a list of Log Encryption Error, see

	VPN book of the FireWall-1 User Guide, Version 4.0	Virtual Private Networks Check Point 2000
Errors Reported by Alice (Encrypting Gateway)	133	259
Errors Reported by Bob (Decrypting Gateway)	136	267
Extended Encryption Protocol (FWZ only)	140	272

SecuRemote Error Messages

For a list of SecuRemote Error Messages, see

- FireWall-1 4.0 Virtual Private Networks, page 101
- Check Point 2000 Virtual Private Networks, page 175